DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 27

[DHS–2006–0073]

RIN 1601–AA41

Chemical Facility Anti-Terrorism Standards

AGENCY: Department of Homeland Security.

ACTION: Advance Notice of Rulemaking.

SUMMARY: Section 550 of the Homeland Security Appropriations Act of 2007 (''Section 550'') provided the Department of Homeland Security with authority to promulgate ''interim final regulations'' for the security of certain chemical facilities in the United States. This notice seeks comment both on proposed text for such interim final regulations and on several practical and policy issues integral to the development of a chemical facility security program.

DATES: Written comments must be submitted on or before February 7, 2007.

ADDRESSES: Comments, identified by docket number or RIN number, may be submitted by one of the following methods:

- Federal eRulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Mail:* Comments by mail are to be addressed to IP/CNPPD/Dennis Deziel, Mail Stop 8610, Department of Homeland Security, Washington DC 20528–8610.

Instructions: All submissions must include the agency name and docket number or Regulatory Information Number (RIN) for this rulemaking. All comments will be posted without change to *http://www.regulations.gov,* including any personal information sent with each comment. For detailed instructions on submitting comments and additional information on the rulemaking process, see the ''Public Participation in Rulemaking Process'' heading of the **SUPPLEMENTARY INFORMATION** section of this document.

Docket: For access to the docket to read background documents or submitted comments, go to *http://www.regulations.gov.* Submitted comments by mail may also be inspected. To inspect comments, please call Dennis Deziel, 703–235–5263, to arrange for an appointment.

Comments that include trade secrets, confidential commercial or financial information, or sensitive security information (SSI) should not be submitted to the public regulatory docket. Please submit such comments separately from other comments on the rule. Comments containing trade secrets, confidential commercial or financial information, or SSI should be appropriately marked as containing such information and submitted by mail to the individual(s) listed in the **FOR FURTHER INFORMATION CONTACT** section.

FOR FURTHER INFORMATION CONTACT: Dennis Deziel, Chief Program Analyst, Chemical Security Regulatory Task Force, Department of Homeland Security, 703–235–5263.

SUPPLEMENTARY INFORMATION:

Introduction

Since 2003, the Department of Homeland Security (DHS) has been working with its private sector partners in the chemical industry, state and local governmental entities and other interested parties on chemical facility security issues. Although many companies in the chemical industry have initiated voluntary security programs and have made significant capital investments in responsible security measures, the Secretary of Homeland Security has concluded that voluntary efforts alone will not provide sufficient security for the nation.

Beginning in 2005, through 2006, and most explicitly on September 8, 2006, the Secretary requested that Congress provide the Department of Homeland Security with regulatory authority to establish and require implementation of risk-based performance standards for the security of our nation's high-risk chemical facilities. Congress took action on those requests, and on October 4, 2006, the President signed the Department of Homeland Security Appropriations Act of 2007 (the Act), which provides the Department of Homeland Security with the authority to regulate the security of high-risk chemical facilities. *See* Pub. L. 109–295, sec. 550. The Department now intends to implement an appropriate regulatory program under Section 550 of that Act as quickly and responsibly as possible, focusing its resources first on those facilities in our nation that present the highest levels of security risk.

This notice discusses a range of regulatory and implementation issues. The program proposed by this notice would be implemented in phases, and DHS would address chemical facilities with the most significant risk profiles as early in the program as possible. For each phase, the program would contain several basic steps:

- Chemical facilities fitting certain risk profiles would complete a ''Top-screen'' risk assessment methodology accessible through a secure Department website. The Department would use this methodology to determine if a chemical facility ''present[s] a high level of security risk'' and should be covered by this program.
- If the Department determines that a chemical facility qualifies as ''high risk,'' the Department would require the facility to prepare and submit a Vulnerability Assessment and Site Security Plan, and would provide technical assistance to the facility as appropriate.
- Following a facility's submission of these materials, the Department would review the submissions for compliance with risk-based performance standards. The Department (or when appropriate, a DHS-certified third-party auditor) would follow up with a site inspection and audit.
- If the facility's Vulnerability Assessment or Site Security Plan is found deficient or if other problems arise, the facility could seek further technical assistance from the Department, and could consult, object, or appeal depending on the stage of the process. If the Vulnerability Assessment and/or Site Security Plan are ultimately disapproved, the covered facility would be required to revise its plan and resubmit the materials to meet the Department's performance standards, or face the penalties and other remedies set forth in the statute.
- If the covered facility's submissions are approved, the security plan is fully implemented and the facility is otherwise in compliance, the Department would issue a Letter of Approval to document the determination. The Department would also then notify the facility of its continuing obligations—based on its level of risk—to maintain and periodically update its Vulnerability Assessment and Site Security Plan.

This advance notice describes the details of these steps along with a number of policy and implementation issues. We seek comment on all aspects of this new regulatory program, including the many policy and practical questions integral to the successful implementation of the program.

Solicitation of Comment

Section 550 requires the Secretary of Homeland Security to promulgate ''interim final regulations establishing risk-based performance standards for security of chemical facilities * * *.'' He must do so ''[n]o later than six months'' from the date of enactment of this new authority, *i.e.* by April 4, 2007. The Executive Branch has implemented rules under other, similar regulatory

authorities over the course of years rather than months. See, *e.g.*, 42 U.S.C. 7412(r)(3) (requiring the promulgation of an initial list of chemicals within two years); 42 U.S.C. 7412(r)(7)(B)(i) (requiring promulgation of regulation within three years). By directing the Secretary to issue ''interim final regulations,'' Congress authorized the Secretary to proceed without the traditional notice-and-comment required by the Administrative Procedure Act. *See, e.g.*, Jeffrey S. Lubbers, A Guide to Federal Agency Rulemaking 114 (4th ed. 2006) (citing Omnibus Budget Reconciliation Act of 1987, and stating that notice and comment is not required where statute specifically permits a regulation to be issued in the interim final form); *see also* 65 FR 34,983 (Jun. 1, 2000) (interim final rule for Medicare program issued under that authority). Although ''interim final regulations'' may be (and often are) issued without prior notice and comment (and the Act requires no prior notice or comment period), the Department believes it would nevertheless be prudent to seek comment on many of the significant issues that will be addressed by such regulations while maintaining the aggressive timeline for implementation. An advance notice of proposed rulemaking is the typical route to seek comment in advance of an NPRM. Here, because Section 550 requires the Secretary to issue an interim final rule rather than an NPRM followed by a final rule, our advance notice seeks comment on text for an upcoming interim final rule. In this respect, this notice serves the purposes usually achieved by both an ANPRM and an NPRM. In addition, it is our intention to seek further comment with the interim final on additional implementation issues, and on any agency guidance that may follow.

The Department seeks public comment from all interested parties by February 7, 2007, on the questions, issues and proposed regulatory language identified in this notice. Given the 6-month deadline under Section 550 to promulgate an interim final rule, it will be necessary to complete that rule and reach conclusions on many of the issues raised herein early in 2007. Thus, this February 7, 2007, deadline cannot reasonably be postponed.

This notice is organized as follows: Section I provides a brief summary of relevant pre-existing Federal initiatives and regulatory authorities; Section II discusses the structure and requirements of the statute; Section III describes a proposed ''phased'' implementation with an immediate priority on the highest risk chemical facilities; and Section IV addresses a range of other legal and programmatic issues.

Table of Contents

I. Brief History of Federal Pre-Existing Chemical Security and Safety Programs

Prior to the enactment of Section 550, the Federal government did not have authority to regulate the security of most chemical facilities. Over the past three years, the Department has urged voluntary enhancement of security at these facilities and provided both technical assistance and grant funding for security. In addition, through the Coast Guard's Maritime Security regulations, the Department has addressed security at certain maritime-related chemical facilities. Recently, the Departments of Homeland Security and Transportation have cooperated in addressing the security of rail transportation of hazardous chemicals.

Other Federal programs have addressed chemical facility safety, but not security: the Environmental Protection Agency (''EPA''), for instance, regulates chemical process safety through its Risk Management Plan (RMP) program; the Occupational Safety and Health Administration (''OSHA'') regulates workplace safety and health at chemical facilities; and the Department of Commerce oversees compliance with the Chemical Weapons Convention. Finally, the Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (''ATF'') regulates, through licenses and permits, the purchase, possession, storage, and transportation of explosives. Because Section 550 will build on pre-existing Federal security initiatives and chemical safety programs, a brief summary of these pre-existing initiatives and programs is appropriate here.

A. DHS Risk Assessment Methodology (RAMCAP), Chemical Buffer Zone Protection Program, and Site Assistance Visits

1. Risk Assessment Methodology (RAMCAP)

For the past two years, the Department has worked with the American Society of Mechanical Engineers, with input from many other parties, to develop a risk assessment methodology for many elements of our nation's critical infrastructure. The methodology is composed of two separate parts and can be utilized to perform both a preliminary ''consequence'' analysis and a more thorough vulnerability assessment on chemical facilities.

The first segment of the RAMCAP methodology is a screening tool known as the Top-screen, and is designed to be used through a secure Department Web site. For chemical facilities, the Top-

screen solicits answers to a series of questions intended to assess the level of damage that could result from a terrorist incident at the facility. The Top-screen process draws in part on preexisting data from the EPA's Risk Management chemical safety program (''RMP,'' discussed below). For example: Does the facility operate any RMP Program 2 or 3 processes? If so, how many persons could be exposed by a toxic release worst case scenario? How many persons could be exposed by a flammable release worst case scenario? The Top-screen also includes queries regarding manufacture and storage of explosives materials, and seeks information on quantities of chemical substances and precursors addressed by the Chemical Weapons Convention. *See* 22 U.S.C. 6701. The Top-screen process is intended to gather information both to evaluate the consequences of a catastrophic explosion or release and to assess the possible danger if dangerous chemicals are stolen. A more detailed description of the Top-screen process is available as Appendix A.

The second segment of RAMCAP provides the tools to conduct a thorough facility Vulnerability Assessment and could also be utilized via a secure website. It has three fundamental steps, each with detailed instructions:

1. Identify the assets on the facility;
2. Apply specified threat scenarios to each asset to quantify the resulting consequences if an attack succeeded; and
3. Apply the threat scenarios to each asset in light of the security measures in place and evaluate the likelihood and the degree to which the attack could succeed.

A detailed description of this process is set forth in Appendix B. Note that many responsible facilities have already conducted analyses of this type. Such analyses may be acceptable during the initial stages of the Section 550 program.

2. Chemical Buffer Zone Protection Program

The Chemical Buffer Zone Protection Program (Chem-BZPP) is designed to identify and implement voluntary protective measures for the area outside of a chemical facility's fence, or the ''buffer zone,'' to make it more difficult for a potential attacker to plan or launch an attack. These plans are intended to develop effective preventive and protective measures within the immediate vicinity of high-priority chemical sector critical infrastructure targets. The plans also increase the security-related capabilities of the jurisdictions responsible for the security and safety of the surrounding communities. DHS provides funds to localities to support the implementation of regional buffer zone plans and mitigate the identified vulnerabilities. In fiscal year (FY) 2006, the Department awarded $25,000,000 under this program.

Part of this effort is the BZPP Webcam Pilot Program, a web-based program using cameras installed at a few high-consequence chemical facilities. These webcams enable local law enforcement and DHS to conduct remote surveillance of the buffer zone surrounding each facility during times of elevated threat to help identify any terrorist surveillance and planning activities and link incidents across facilities.

3. Site Assistance Visits

Upon request, DHS conducts ''inside-the-fence'' site assistance visits to critical chemical facilities for a variety of reasons—a facility presents a high level of risk, the owner requests it, or the facility or sector is under threat. The site visits are conducted by DHS protective security professionals, subject-matter experts, and local law enforcement, along with the facility's owners and operators. These visits facilitate security vulnerability identification and mitigation discussions between government and industry. The visits also provide facilities and localities with valuable information on how to better protect the facility from a terrorist attack. After a visit, DHS suggests protective measures and issues a report to the facility to bolster its protective measures.

B. U.S. Coast Guard Maritime Security Regulations

The Maritime Transportation Security Act of 2002 (MTSA) (Pub. L. 107–295, Nov. 25, 2002) enacted chapter 701 of Title 46, U.S. Code and required the Secretary of Homeland Security to issue regulations to strengthen the security of American ports and waterways and the ships that use them. This authority, in addition to other grants of authority, served as the basis for a comprehensive maritime security regime. Through these rules, the Coast Guard issued regulations to ensure the security of vessels, facilities, and other elements of the maritime transportation system. Part 105 of title 33 of the Code of Federal Regulations imposed requirements on a range of maritime facilities, including hazardous material and petroleum facilities and those fleeting facilities that receive barges carrying, in bulk, cargoes regulated by Subchapters D and O of Chapter I, Title 46, Code of Federal Regulations or Certain Dangerous Cargoes.

Under the Coast Guard's maritime security regulations, these facilities are required to perform security assessments, and then, based on these assessments, develop security plans, and implement security measures and procedures in order to reduce the risk of and to mitigate the results of any security incident that threatens the facility, its personnel, the public, the environment, and the economy.

C. Rail Security

The Departments of Transportation (DOT) and Homeland Security both have authority to regulate rail transportation. The Federal hazardous materials transportation law authorizes the Secretary of Transportation to establish regulations for the safe transportation, including security, of hazardous materials in intrastate, interstate, and foreign commerce. *See* 49 U.S.C. 5101 et seq., as amended by section 1711 of the Homeland Security Act of 2002 (Pub. L. 107–296, Nov. 25, 2002) and Title VII of the Safe, Accountable, Flexible and Efficient Transportation Equity Act: Legacy for Users (SAFETEA–LU) (Pub. L. 109–59, Aug. 10, 2005). DHS, through TSA, has authority to ''oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities.'' 49 U.S.C. 114(f)(11).

Pursuant to DOT's authority, the Pipelines and Hazardous Materials Safety Administration (PHMSA) has issued, and the Federal Railroad Administration (FRA) enforces, various regulations that impact rail security. HM–232 requires covered persons—those who offer certain hazardous materials for transportation in commerce and those who transport certain hazardous materials in commerce—to develop and implement security plans. At a minimum, these security plans for transportation must address personnel security, unauthorized access for the transportation-related areas of facilities, and en route security for shipments of the covered hazardous materials. *See* 49 CFR 172.800, 172.802, and 172.804. In addition, PHMSA has issued regulations to reduce the risks to safety and security of leaving loaded rail cars unattended for periods of time. Pursuant to 49 CFR 174.14 and 174.16, a carrier must forward each shipment of hazardous materials ''promptly and within 48 hours (Saturdays, Sundays, and holidays excluded)'' after the carrier accepts the shipment at the originating point or the carrier receives the

shipment at any yard, transfer station, or interchange point.

Together with the Department of Transportation, DHS has recently taken many steps regarding security in the transportation of hazardous materials by rail. On June 23, 2006, DOT and DHS jointly issued a set of twenty-four ''security action items'' for the freight rail carriers of materials that are ''toxic by inhalation'' (TIH) (these materials are also referred to as ''poisonous by inhalation'' (PIH)). DOT and DHS, in consultation with the industry, developed these action items by observing and assessing the security-related practices that rail carriers use. The action items addressed three phases of security: (1) System Security, (2) En-route Security, and (3) Access Control.

In August 2006, the Federal government and the industry agreed upon ''supplemental'' security action items including measures to address four critical areas: (1) The establishment of secure storage areas for rail cars carrying TIH materials, (2) the expedited movement of trains transporting rail cars carrying TIH, (3) the positive and secure handoff of TIH rail cars at point of interchange and at points of origin and delivery, and (4) the minimization of unattended loaded tank cars carrying TIH materials. The rail carriers will submit these plans to TSA for review, and TSA will subsequently monitor and evaluate the success of the plans in reducing the standstill (dwell) time of TIH shipments in high threat urban areas.

On December 21, 2006, DOT and TSA issued notices of proposed rulemaking that would impose additional obligations, including new requirements regarding transportation of PIH materials. See DOT's notice of proposed rulemaking titled ''Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments'' at 71 FR 76834 and TSA's notice of proposed rulemaking titled ''Rail Transportation Security'' at 71 FR 76851. The proposed regulations would cover railroad carriers that transport certain hazardous materials, including bulk shipments of PIH materials. Among other measures, the proposed DOT rule would require railroad carriers to analyze the safety and security risks of the routes used. It would also require clarifications of the current security plan requirements to address en route storage, delays in transit, and delivery notification. In addition, it would require rail carriers to conduct pre-trip visual inspections at the ground level of rail cars containing PIH materials to detect improvised explosive devices (IEDs) or other evidence of tampering.

The proposed TSA rule would require those rail hazardous materials shippers and receivers, along with freight and passenger railroad carriers and rail transit systems, to (1) Designate a rail security coordinator to serve as the primary contact for the receipt of intelligence information and for other security-related activities; (2) allow TSA and other authorized DHS officials to enter and inspect property, facilities, equipment, and operations; and (3) report incidents, potential threats, and significant security concerns to DHS. In addition, TSA proposes to impose two additional requirements on PIH rail hazardous materials shippers and receivers, as well as freight railroad carriers that transport PIH: to (1) Provide to TSA, upon request the location and shipping information of rail cars within their physical custody or control that contain PIH materials, and (2) provide for a secure chain of custody and control of rail cars that contain PIH materials.

D. Environmental Protection Agency Risk Management Program

Pursuant to the Clean Air Act (CAA), EPA's Risk Management Program requires chemical facilities with listed chemicals in amounts exceeding prescribed threshold limits to implement an accident prevention program, an emergency response program, prepare a five-year accident history, and submit to EPA a risk management plan (RMP). *See* 42 U.S.C. 7412(r). These requirements are intended to prevent accidental releases and minimize the consequences of such releases by focusing on chemicals that in the event of an accidental release, could reasonably be expected to cause death, injury, or serious adverse effects to human health and the environment. On January 31, 1994, EPA promulgated a list of regulated substances and thresholds that identify stationary sources subject to the accidental release prevention regulations. 59 FR 4,478. Two years later, EPA issued a rule requiring the owners of these sources to develop accidental release programs and summaries of these plans. 61 FR 31,668 (Jun. 20, 1996).

An RMP contains information on the regulated substances handled at the facility, an analysis of the potential consequences of hypothetical accidental chemical releases (i.e., ''worst-case'' and ''alternative release'' scenarios), a five-year accident history, and information about the chemical accident prevention and emergency response programs at the facility. In 1999, more than 15,000 U.S. facilities submitted RMP information to EPA. Regulated facilities are required to update their RMPs at least every five years, and more frequently if specified changes occur.

As the RMP chemical list and threshold limits were established by EPA based on a chemical's potential for acute offsite health impacts in the event of a large air release, the Department believes that a number of the facilities regulated under this program may also qualify as ''high-risk'' facilities covered under Section 550. Although the RMP data are extremely useful, the Department is mindful of the fact that they contain information related only to a specified list of industrial chemicals that present air release hazards. The RMP data do not provide information relating to other potentially ''high-risk'' facilities, such as certain facilities covered by the Chemical Weapons Convention or certain other facilities that might be targeted for chemical theft or diversion.

E. Occupational Safety and Health Administration

The Occupational Safety and Health Administration (OSHA), an agency within the U.S. Department of Labor, regulates conditions and hazards affecting the health and safety of employees in the workplace. OSHA's mission is to prevent work-related injuries, illnesses, and deaths. OSHA regulates employers through specific enumerated safety standards (*see, e.g.*, 29 CFR part 1910) and through a ''general duty clause'' (*see* 29 U.S.C. 654(a)(1)), which requires a safe workplace even in the absence of specific standards. OSHA enforces these standards by inspecting workplaces and by issuing citations for violations.

OSHA has developed and enforces several standards that ensure chemical safety in the workplace. The Process Safety Management of Highly Hazardous Chemicals standard contains requirements for the management of hazards associated with processes using highly hazardous chemicals. *See* 29 CFR 1910.119. The Hazardous Waste Operations and Emergency Response Standard (HAZWOPER) covers emergency response operations for the release of, or substantial threats of releases of, hazardous substances without regard to the location of the hazard. *See* 29 CFR 1910.120 and 1926.65.

In addition, OSHA has several other regulations that protect employees who are exposed to chemicals in the course of their work. In Subpart Z to 29 CFR 1910, OSHA establishes permissible exposure limits (PELs) for toxic and hazardous substances. Employers must measure employee exposure to these

substances and must take measures to limit employee exposures when the exposures reach impermissible limits. In Subpart I to 29 CFR 1910, OSHA establishes requirements for personal protective equipment (PPE). Employers must conduct hazard assessments. Where employees are exposed to impermissible exposures (which may, in some cases, be chemical exposures), employers must provide employees with proper PPE to assist in controlling the hazard.

Another standard related to chemical safety is OSHA's Hazard Communication Standard (HCS). The HCS was promulgated to provide workers with the right to know the hazards and identities of the chemicals they are exposed to while working, as well as the measures they can take to protect themselves. The HCS requires chemical manufacturers and importers to evaluate the hazards of the chemicals they produce and import. It also requires chemical manufacturers and importers to prepare labels and material safety data sheets (MSDSs) to convey the hazard information to their downstream customers. All employers with hazardous chemicals in their workplaces must have labels and MSDSs for their exposed workers and must train exposed workers to handle the chemicals appropriately. *See* 29 CFR 1910.1200.

F. Chemical Weapons Convention

The United States is a party to the Chemical Weapons Convention (CWC), which prohibits the development, production, stockpiling, and use of chemical weapons. The Convention entered into force on April 29, 1997, and was implemented in the United States by statute at 22 U.S.C. 6701 *et. seq.*, with regulations at 15 CFR 710 *et. seq.* The CWC does not prohibit production, processing, consumption, or trade of related chemicals for peaceful purposes, but it does establish a verification regime to ensure such activities are consistent with the object and purpose of the treaty. The CWC requires reporting and on-site inspections that are triggered when quantitative threshold activity levels are exceeded. The CWC monitors chemicals in three lists, or schedules, and certain ''unscheduled discrete organic chemicals.''

Schedule 1 includes toxic chemicals with few or no legitimate uses that are developed or used primarily for military purposes. Examples of schedule 1 chemicals include nerve agents, such as Sarin, and blister agents, such as Mustard and Lewisite. Schedule 2 includes chemicals that can be used for chemical weapons production, but that also have certain legitimate uses. Schedule 2 chemicals are not produced in large commercial quantities, and these include certain chemicals used to manufacture fertilizers and pesticides. Schedule 3 chemicals are those that can be used for chemical weapons production, but also have significant legitimate uses. Schedule 3 chemicals are produced in large commercial quantities and include chemicals used to manufacture paint thinners, cleaners, and lubricants.

As noted, the CWC imposes declaration and on-site inspections requirements upon industry when production, processing, or consumption exceeds certain thresholds. Inspections under the CWC are conducted to assess the risk and guide future routine inspections. In addition, inspections are conducted to verify the consistency with the declarations of the levels of production, processing, or consumption. These inspections also seek to confirm the absence of undeclared Schedule 1 chemicals.

G. The Explosives Authority of the Bureau of Alcohol, Tobacco, Firearms, and Explosives

ATF is an enforcement and regulatory organization responsible for, among other things, the investigation and prevention of Federal offenses involving the unlawful use, manufacture, and possession of explosives. ATF regulates, through licenses and permits, the purchase, possession, storage, and transportation of explosives. *See generally* 27 CFR Part 555. Specifically, ATF explosives regulations govern commerce; licensing of manufacturers, importers, and dealers; issuance of permits; business by licensees and operations by permittees; storage; and the records and reports required of licensees and permittees. 27 CFR 555.1. Each year, ATF issues the List of Explosives subject to these explosives requirements. *See, e.g.*, 70 FR 73,483 (Dec. 12, 2005).

Facilities that possess or store explosives (including manufacturing facilities) must also be properly licensed by ATF. *See* 27 CFR 555.41 *et seq.* For facilities that possess or store listed explosives, ATF requires certain safety precautions, including specific requirements governing the actual storage of the materials. *See* 27 CFR 555.201 *et seq.* ATF also prohibits shipment, transport, or possession of any explosive material by ''prohibited persons,'' including a person under indictment or convicted of a crime punishable by imprisonment for a term exceeding one year; a fugitive from justice; an unlawful user of controlled substance; or ''has been adjudicated a mental defective.'' *Id.* at 555.26(c), 555.49. ATF may conduct an investigation to confirm that an applicant is entitled to a license. *Id.* ATF will also conduct a background check on all persons and employees who are authorized to possess explosive materials as part of their employment. *See* 27 CFR 555.33.

II. Structure and Requirements of Section 550

With the authority under Section 550, the Department can now fill a significant security gap in the country's anti-terrorism efforts. Section 550 of the Act is a compact two-page set of mandates establishing the parameters of the Federal government's first regulatory program to secure chemical facilities against possible terrorist attack. Each subsection and sentence of this provision has significant consequences for the structure and content of the regulatory program.

*A. The Mandate to Promulgate Interim Final Regulations ''No later than six months after the date of enactment * * *''*

As discussed above, applicable statutes do not require the Department to seek comment prior to issuing these regulations, but we believe public comment will be very helpful in formulating the interim final rule and structuring the program. *Cf.* Administrative Conference of the United States Recommendation 76–5 (when it is necessary to make a rule effective immediately, agencies should give the public the opportunity to submit post-promulgation comments) (cited in Michael Asimow, *Nonlegislative Rulemaking and Regulatory Reform*, 1985 Duke L.J. 381, 426). An interim final rule has the same legal effect as a final rule. *See, e.g.*, *Career College Ass'n* v. *Riley*, 74 F.3d 1265, 1268 (D.C. Cir. 1996) (stating that interim final rule is final for purposes of statute requiring adoption of final rule by statutory date). In this regard, this notice discusses a number of issues related to promulgating chemical facility security regulations and invites comments on these issues. This notice includes proposed regulatory text which represents the Department's initial preference unless otherwise identified, but the Department also seeks comment on proposals and ideas discussed in the preamble but not contained in the regulatory text because the Department is interested in comments on alternative approaches.

The Department is currently considering a number of procedural questions that relate to the authority it has been granted. An initial question is whether the Department is required to finalize the interim regulations in light of the express language of 550(b), which provides that these interim regulations will apply until ''interim or final regulations promulgated *under other laws*'' are in effect. Pub. L. 109–295, Oct. 4, 2006 (emphasis supplied). We believe that the answer to that question is no; Congress gave the Department the authority to issue regulations in the interim final rule only; it did not contemplate that such regulations be ''finalized'' under this authority. It is important to note that these ''interim'' regulations will nevertheless have the full effect of law as if they were final. *See e.g.*, *Career College Ass'n* v. *Riley*, 74 F.3d 1265, 1268 (D.C. Cir. 1996).

A second issue is whether the Department can revise the interim final regulations issued under Section 550. Commentators have argued that the regulations cannot be revised since 550(a) and (b) indicate that the regulations must be issued ''no later than six months after the date of enactment'' and ''shall apply until'' the end date contemplated by Section 550(b). We believe the better view is that the regulations can be revised after the six month timeframe.

A third issue is what type of future legislation is necessary to replace the interim final rule under Section 550(b). Certainly, Section 550 could be superseded or extended in either an appropriations bill or in authorization legislation. If a future appropriations bill continued funding for the Section 550 program beyond that period, the Department could consider that future funding for the program as an extension of the ''authority provided by this section.''

B. Authority To Regulate ''Chemical Facilities'' that Present a ''High Level of Security Risk''

A fundamental question posed by Section 550 is which facilities it covers. Section 550 specifies that the provision ''shall apply to chemical facilities that, in the discretion of the Secretary, present high levels of security risk.'' The terms ''chemical facilities'' and ''high levels of security risk'' are not specifically defined in Section 550. Both terms have, however, been used in two prior legislative proposals with more explicit indications of their meaning. *See* H.R. 5695, 109th Cong. (2006), S. 2145, 109th Cong. (2006). Although the Department is not bound to interpret these terms in concert with language of prior unenacted legislative proposals, those prior proposals can provide helpful context on this specific definitional issue.

In H.R. 5695, the term ''chemical facility'' refers to any facility that the Secretary has determined to possess more than a threshold amount of a potentially dangerous chemical. *See* H.R. 5695, 109th Cong. sec. 2 (2006) (adding section 1802(b)(2) and subsequent sections in the Homeland Security Act). (S. 2145 uses different terms to a similar effect.). In neither instance is a ''chemical facility'' limited to a chemical manufacturing facility, a chemical distribution facility, or any other single specific type of facility that uses or stores potentially dangerous chemicals. Instead, the question of what constitutes a chemical facility turns not on the name or type of facility at issue, but instead on whether the facility uses, stores or otherwise possesses dangerous chemicals, and in what amount. The Department believes that a similar meaning of ''chemical facility'' is appropriate in implementing Section 550. Thus, subject to certain statutory exclusions which are discussed below in section II.L., the Department proposes to define ''chemical facility'' as ''any facility that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criterion identified by the Department.'' *See* proposed 6 CFR 27.100. We invite comment specifically on this interpretation or any alternative definitions of the term ''chemical facility.''

Of course, the term ''chemical facility'' is only significant in relation to other text in the statute. Section 550 also specifies that regulations promulgated under its authority are only applicable to a ''chemical facility'' that, ''in the discretion of the Secretary, presents [a] high level[] of security risk.'' Not all chemical facilities present a high level of security risk. (Indeed, not all ''chemical facilities'' on the RMP list are likely to present a high level of security risk.) Both H.R. 5695 and S. 2145 had specific provisions distinguishing the universe of all ''chemical facilities'' from the subset of ''high risk'' chemical facilities. H.R. 5695 would have required that ''at least one of the tiers established by the Secretary for the assignment of chemical facilities * * * shall be a tier designated for high-risk chemical facilities.'' 109th Cong. sec. 2 (2006) (proposed 6 U.S.C. 1802(c)(4)). Similarly, although S. 2145 identified the regulated chemical facilities as those with chemical substances of concern at sufficient threshold quantities, that bill also contained an instruction for the Secretary to identify separately a smaller subset of those facilities as high risk chemical facilities. S. 2145, 109th Cong. sec. 3(e) (2006). Thus, in both prior legislative proposals, Congress contemplated that only a subset of all facilities with threshold quantities of certain chemical substances would also qualify as ''high risk'' chemical facilities.

The Department believes that the phrase ''high level of security risk'' in Section 550 was likewise intended to apply only to a subset of the total population of ''chemical facilities.'' Under Section 550, the Secretary is explicitly given discretion to determine which chemical facilities fall within this subset, and thus which chemical facilities the Department will regulate. *See* Pub. L. 109–295, sec. 550(a) (2006) (''such regulations shall apply to chemical facilities that, in the discretion of the Secretary, present high levels of security risk''). *See also* 5 U.S.C. 701(a)(2) (precluding judicial review if ''agency action is committed to agency discretion by law''). *See also Webster* v. *Doe*, 486 U.S. 592 (1988); *Heckler* v. *Chaney*, 470 U.S. 821, 830 (1985) (recognizing the exception to the presumption of agency reviewability in 5 U.S.C. 701(a)(2)); *Steenholdt* v. *FAA*, 314 F.3d 633 (D.C. Cir. 2003); *Baltimore Gas & Elec. Co.* v. *FERC*, 252 F.3d 456, 459 (D.C. Cir. 2001); *Haig* v. *Agee*, 453 U.S. 280 (1981); *Merida Delgado* v. *Gonzales*, 428 F.3d 916 (10th Cir. 2005) (finding that the Attorney General's national security determination was not reviewable under the APA, where the authorizing statute provided no meaningful standard against which to judge the agency's action, the court did not have the necessary expertise to make the determination, and the Executive Branch has broad discretion to protect national security).

C. Determining Which Facilities Present a High Level of Security Risk

As a practical matter, the Department must utilize an appropriate process to determine which facilities present sufficient risk to be regulated. The Department may draw on many sources of available information, including existing Federal data and lists addressing particularly hazardous chemicals and particular chemical facilities. Such lists include the EPA RMP list (discussed above); the schedule of chemicals from the Convention on the Development, Production, Stockpiling and Use of Chemical Weapons and Their

Destruction, also known as the Chemical Weapons Convention or CWC (discussed above); the hazardous materials listed in Department of Transportation's Hazardous Materials Regulations (*see e.g.* 49 CFR 172.101); and the TSA Select Hazardous Materials List. The Department may also seek and analyze information from many other sources, including from experts in the industry, from state or local governments or directly from facilities that may qualify as high-risk. The Department requests comment on appropriate sources of information or methodologies for evaluating chemical facility risks. The Department also requests comments on whether, to the extent it looks to the nature of particular chemicals to classify facilities, classifications should be based on a ''hazard-class'' approach rather than classifications based on particular chemicals.

As discussed above, the Department has worked with the American Society of Mechanical Engineers (ASME) and others to design a RAMCAP ''Top-screen'' process for determining the potential security risk posed by many types of critical infrastructure facilities, including chemical facilities. The Department proposes to employ a risk assessment methodology system very similar to this RAMCAP Top-screen process to determine whether a facility qualifies as high-risk under Section 550, and seeks comment on how such a process—as described above and in Appendix A—should be employed for that purpose.

The proposed regulation would permit the Department to implement this type of Top-screen risk analysis process to screen facilities. The proposed language interprets the statutory phrase ''present[s] high levels of security risk'' to apply to a facility that, in the discretion of the Secretary, would present a high risk of significant adverse consequences for human life or health, national security or critical economic assets if subjected to a terrorist attack. *See* proposed 6 CFR 27.100, below. As noted, the statute gives the Secretary unreviewable discretion to make this determination. *See* Pub. L. 109–295, secs. 550(a), (b), Oct. 4, 2006.

A separate question is whether the Secretary can compel facilities that have not yet been deemed ''high risk'' to complete a risk assessment methodology such as the RAMCAP Top-screen, or punish them for failure to do so. In other words, can the Secretary mandate information submissions from a broad range of chemical facilities in order to screen facilities and determine which will qualify as high risk?

There are two arguments that the Secretary has such authority under Section 550. First, the authority to determine which facilities qualify as ''high risk'' implies necessary authority to obtain information to make that determination. *See, e.g., United States* v. *Construction Products Research, Inc.*, 73 F.3d 464, 470 (2d Cir. 1996) (''at the subpoena enforcement stage, courts need not determine whether the subpoenaed party is within the agency's jurisdiction or covered by the statute it administers''); *Equal Employment Opportunity Commission* v. *Sidley Austin Brown & Wood*, 315 F.3d 696, 699–701 (7th Cir. 2002). Second, Section 550 states explicitly that the Secretary ''shall audit and inspect chemical facilities for the purposes of determining compliance with the regulations issued pursuant to this section.'' Since this provision can be read to permit the Department physically to inspect ''chemical facilities'' regardless of whether they qualify as ''high risk,'' the Department should impliedly have the less dramatic authority to obtain preliminary information for the same purpose. Indeed, the use of a Top-screen process will be a less onerous imposition for many facilities that may not, after due consideration, present high levels of security risk.

The following approach to screening facilities is reflected below in the proposed rule text:

- The Department could contact chemical facilities individually to request that they complete the process and could publish a notice requesting that all facilities fitting a certain profile (based on quantity of certain chemicals on site, hazard classification, or other criteria) complete an online Department risk assessment methodology (similar to the RAMCAP Top-screen) within a reasonable period.
- If any facility fitting the profiles identified in the notice or individually contacted by the Department fails to complete the risk assessment methodology within a reasonable period of time after receiving notification from the Department, the Department may, after attempting to consult with the facility, reach a preliminary determination, based on the information then available (which may include the facility's failure to complete the Top-screen process), that the facility ''presumptively presents a high level of security risk.''
- The Department would then issue a notice to the entity of this determination and, if necessary, order the facility to complete the Top-screen process. If the facility then fails to do so, it may be subject to penalties pursuant to Section 550(d), audit and inspection under Section 550(e) or, if appropriate, the remedy available under Section 550(g). *See proposed § 27.305, 245, 310.*
- If the facility completes the Top-screen process and is not then considered to present a high level of security risk, its status as ''presumptively high risk'' will terminate, and the Department will issue a notice to the facility to that effect.

The Department requests comments on this proposed process and the draft regulation at §§ 27.200 and 27.205 below.

In order to carry out this approach, the Department will need to identify the types or classes of facilities that should complete Top-Screen for screening purposes. To that end, the Department requests comments on whether the Department should request that:

- RMP facilities complete the Top-screen;
- Certain facilities subject to the Chemical Weapons Convention complete the Top-screen;
- Any other type or description of facilities complete the Top-screen.

The Department also anticipates permitting any chemical facility to voluntarily complete the Top-screen risk assessment process if the facility has not been notified or contacted by DHS for such screening.

D. Risk-Based Performance Standards for Security of Chemical Facilities

Among other things, Section 550 requires the Department to issue interim final regulations ''establishing risk-based performance standards for chemical facilities.'' The terms ''risk-based'' and ''performance standards'' both carry significant meaning.

The term ''performance standards'' has a long and well-known history. *See* Cary Coglianese et al., *Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection*, 55 Admin. L. Rev. 705, 706–07 (2003). The term has repeatedly been defined: Performance standards

* * * state[] requirements in terms of required results with criteria for verifying compliance but without stating the methods for achieving required results. A performance standard may define functional requirements for the item, operational requirements, and/or interface and interchangeability characteristics. A performance standard may be viewed in juxtaposition to a prescriptive standard which may specify design requirements, such as materials to be used,

how a requirement is to be achieved, or how an item is to be fabricated or constructed.

OMB Circular A–119 (Feb. 10, 1998); *see also* Coglianese, *Performance-Based Regulation*, 55 Admin. L. Rev. at 709:

A performance standard specifies the outcome required, but leaves the specific measures to achieve that outcome up to the discretion of the regulated entity. In contrast to a design standard or a technology-based standard that specifies exactly how to achieve compliance, a performance standard sets a goal and lets each regulated entity decide how to meet it.

Note also that Executive Order 12,866 specifies the use of performance standards:

Each agency shall identify and assess alternative forms of regulation and shall, to the extent feasible, specify performance objectives, rather than specify the behavior or manner of compliance that regulated entities must adopt.

Exec. Order 12,866, 58 FR 51,735 (Oct. 4, 1993), as amended by Exec. Order 13258, 67 FR 9385 (Feb. 28, 2002).

Here, Section 550 specifies that the required ''performance standards'' must be ''risk-based.'' Although the term ''risk-based'' is not specifically defined in Section 550, the language of Section 550 along with other recent legislative activity yield an understanding of the ''risk-based'' standards. The term ''risk-based'' modifies ''performance standard'' and indicates that the performance standards established under Section 550 will mandate the most rigorous levels of protection and regulatory scrutiny for facilities that present the greatest degrees of security risk. Prior legislative proposals on chemical security would have required this result expressly through risk-based tiering of facilities based on the potential affects on human health caused by a terrorist attack at a facility, potential impact on national security, or potentially critical economic consequences. *See* H.R. 5695, 109th Cong. sec. 2 (2006), S. 2145, 109th Cong. (2006). In many of those prior proposals, the Department would have been required to analyze relative risk first, sort facilities into appropriate risk-based tiers, then create standards requiring more robust levels of protection for higher risk tiers. In addition, prior legislative proposals specified more frequent regulatory reviews, inspections, and security plan updates for higher risk facilities.

The Department believes that the ''risk-based performance standards'' and the Section 550 Program should indeed incorporate risk-based tiering. As addressed above, Section 550 provides the Department with authority to regulate those chemical facilities ''that, in the discretion of the Secretary, present high levels of security risk.'' Thus, the risk-based tiers would differentiate and create tiers among those facilities that, as described above, qualify as presenting ''high levels of security risk'' and are thus ''covered facilities.'' The Department seeks comment on this notion of risk-based tiering among high-risk facilities. Specifically:

- How many risk-based tiers should the Department create?
- What should be the criteria for differentiating among the tiers?
- What types of risk should be most critical in the tiering?
- How should the performance standards differ among risk-based tiers?
- What additional levels of regulatory scrutiny (e.g. frequency of inspections, plan reviews, and updates) should apply to each tier?

The Department would establish the risk-based performance standards through the regulatory language below and intends to issue guidance periodically regarding compliance with the standards. Please note that specific security performance variables in the standards among tiers for the covered facilities are likely to contain sensitive information regarding covered facility vulnerability or security. Thus, certain elements of guidance on the application of these standards by tier will be provided to covered facilities pursuant to the information protections provisions of Section 550.

E. Vulnerability Assessments and the Development and Implementation of Site Security Plans for Chemical Facilities

The first sentence of Section 550 requires the Department to mandate that ''high risk'' chemical facilities, known here as ''covered facilities,'' perform Vulnerability Assessments and develop and implement Site Security Plans.

1. Vulnerability Assessments

A Vulnerability Assessment is an examination of how a covered facility would address specific types of possible terrorist threats. The assessment also examines the aspects of the covered facility that pose the most significant vulnerabilities to terrorist attack. The Department has worked with its partners to develop a methodology for this purpose which may be refined to fit the needs of this program's Vulnerability Assessment program. The methodology is described in detail in Appendix B. The Department seeks comment on how this methodology should be refined to serve as a basis for Vulnerability Assessments under Section 550.

Covered facilities, those that qualify as ''high risk'' under Section 550, will be required to complete and submit Vulnerability Assessments. DHS will review each Vulnerability Assessment, and the Department may also scrutinize the Vulnerability Assessments in the course of a facility audit (discussed *infra*). In addition, a covered facility Vulnerability Assessment will serve two other central purposes: (1) The Department will use the results of Vulnerability Assessments to confirm that covered facilities have been assigned to the appropriate risk-based tiers; and (2) Each covered facility's Site Security Plan (discussed below) will be required to address each of the vulnerabilities identified in the Vulnerability Assessment. *See* Pub. L. 109–295, sec. 550(a), Oct. 4, 2006 (''Provided further, That such regulation shall permit each facility, in developing and implementing Site Security Plans, to select layered security measures that, in combination, appropriately address the Vulnerability Assessment and the risk-based performance standard for security for the facility.'') Covered facilities also have continuing obligations, which vary based on their risk-based tier, to maintain and periodically update their Vulnerability Assessment.

As noted, the Department will sort the covered facilities into tiers, based on risk. The Department may have three or four tiers, with the highest risk facilities in tier one. The tiering decisions will be based on a number of factors, including information from the Top-screen, intelligence information, and information from other appropriate sources. As discussed below in a section II. K., the Department considers the methods for determining these tiers to be sensitive anti-terrorism information that may be protected from further disclosure.

Many chemical facilities have already performed Vulnerability Assessments under models that are similar in purpose and effect to the RAMCAP methodology identified above. For a number of covered facilities, particularly in the initial year of the program, these Vulnerability Assessments will be acceptable in lieu of completing the Department's vulnerability analysis. Through the Alternative Security Program (ASP) provisions described herein, the proposed regulation will permit the Assistant Secretary to accept existing chemical facility Vulnerability Assessments, subject to any necessary revisions or supplements, where the

assessments are sufficiently similar to the Department's process to be effective. The Department is considering accepting any Vulnerability Assessments methodologies that are certified by the Center for Chemical Process (CCPS) as equivalent to the CCPS Methodology; and will review other Vulnerability Assessments submitted as ASPs. See proposed 6 CFR 27.215(a).

2. Site Security Plans

Under Section 550, the Department must also require that ''high risk'' chemical facilities develop and implement ''Site Security Plans.'' The statute specifies that the Department ''shall permit each facility, in developing and implementing Site Security Plans, to select layered security measures that, in combination, appropriately address the Vulnerability Assessment [for the facility] and the risk-based performance standards for security for the facility.'' This sentence identifies two critical statutory mandates.

First, as indicated, a Site Security Plan must address both the ''Vulnerability Assessment'' for the covered facility and the applicable ''risk-based performance standards.'' To address the Vulnerability Assessment, the plan must identify and describe the function of the measures the covered facility will employ to address each of the facility's vulnerable areas. Focusing on those vulnerable areas, the Site Security Plan must then address specific modes of potential terrorist attack and how each would be deterred or otherwise addressed. For example, a facility must select, develop and describe security measures intended to address potential attacks involving: (1) A VBIED (vehicle borne improvised explosive device); (2) a water-borne explosive device (if applicable); (3) an assault team; (4) individual(s) on the premises with explosives or a firearm, or (5) theft of certain chemicals; and (6) the possibility of insider or cyber sabotage.

In addition, a covered facility's Site Security Plan must identify how the layered security measures selected by the covered facility meet the Department's risk-based performance standards. Although this process can be different for each facility and will vary depending on the unique risks presented in each, the performance standards will typically require covered facilities to develop and explain security measures to:

- Secure and monitor the perimeter of the facility;
- Secure and monitor restricted areas or potentially critical targets within the facility;
- Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals, deliveries, and vehicles as they enter; including,
  - Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and
  - Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures;
- Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
- Secure and monitor the shipping and receipt of hazardous materials from the facility;
- Deter theft or diversion of potentially dangerous chemicals;
- Deter insider sabotage;
- Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, Supervisory Control And Data Acquisition (SCADA) systems, and other sensitive computerized systems;
- Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;
- Maintain effective monitoring, communications and warning systems, including,
  - Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;
  - Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and
  - Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;
- Ensure proper security training, exercises, and drills of facility personnel;
- Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or potentially critical targets;
- Escalate the level of protective measures for periods of elevated threat;
- Address specific threats, vulnerabilities, or risks identified by the Assistant Secretary for the particular facility at issue;
- Report significant security incidents to the Department;
- Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;
- Establish official(s) and an organization responsible for security and for compliance with these standards;
- Maintain appropriate records; and
- Address any additional performance standards the Assistant Secretary may specify.

The types and intensity of measures necessary to satisfy these standards will depend, of course, on the risk-based tier of the covered facility at issue. Covered facilities will also have a continuing obligation, which will vary based on their risk-based tier, to maintain and periodically update their Site Security Plan.

Aside from the performance standards identified in proposed § 27.230, the Department will also consider adopting other performance standards from the following meriting security regulatory provisions: 33 CFR 105.250 (Security systems and equipment maintenance); 33 CFR 105.255 (Security measures for access control); 33 CFR 105.260 (Security measures for restricted areas); 33 CFR 105.275 (Security measures for monitoring); 33 CFR 105.280 (Security incident procedures). The terms of these provisions, if adopted, would need modification. For example, the provisions related to security measures for restricted areas identifies such areas to include ''[s]hore areas immediately adjacent to each vessel moored at the facility.'' 33 CFR 105.260. The Department requests comments on whether these or other MTSA regulatory provisions should be adopted in modified form. The Department also requests specific comments on how, if adopted, the Department should modify these provisions.

Section 550 also strikes a careful balance between the Department's regulatory authority and a covered facility's discretion to select security measures. Three separate provisions are relevant to this balance. As noted above, the term ''performance standards'' has long been defined to ''specif[y] the outcome required, but leave[] the specific measures to achieve that outcome up to the discretion of the regulated entity.'' See above, Coglianese, *Performance-Based Regulation*, 55 Admin. L. Rev. at 709. The statute also mandates that the Department ''*shall*

permit each facility * * * *to select* layered security measures * * * '' to address its vulnerabilities and the performance standards. Pub. L. 109–295, sec. 550(a), Oct. 4, 2006 (emphasis supplied). Further, the statute specifically prohibits the Department from rejecting a Site Security Plan, because it does not incorporate a specific type of security measure: ''[T]he Secretary *may not* disapprove a Site Security Plan submitted under this section based on the presence or absence of a particular security measure.'' *Id.* (emphasis supplied).

The meaning of these three provisions was not in dispute at the time of Congress's Conference on the Appropriations Bill on September 29, 2006. Indeed, as Representative Markey and others noted, ''the Department of Homeland Security is prohibited from disapproving of a facility's security plan because of the absence of any specific security measure.'' *See* 152 Cong. Rec. H7907 at H7913 (daily ed. Sept. 29, 2006).

Although the Department may not require that a covered facility select a specific measure to enhance its security, the Department may ''disapprove a Site Security Plan if [the plan] fails to satisfy the risk-based performance standards established by this section.'' Pub. L. 109–295, sec. 550(a), Oct. 4, 2006. The Department understands Section 550 to require a fairly straightforward process: The Department may disapprove a Site Security Plan for failing to satisfy the risk-based performance standards, but may not mandate that the covered facility cure the deficiency by implementing one particular security solution. In other words, the Department cannot take the position that only one type of action or measure can meet the performance standards. Nor can the Department indirectly compel the covered facility to choose a particular measure preferred by the Department by ruling out all other possible alternatives. (Thus, the Department may not engineer the performance standards to permit only one actual security option for a covered facility.) In practical terms, this means that covered facilities will have the opportunity to determine how to remedy a deficient plan. Thus, following a Site Security Plan ''disapproval,'' the Department will permit the covered facility to select a different and more robust combination of security measures and present its plan again. The Department will then judge the revised resubmitted plan against the performance standards. The covered facility must meet the security outcome required in the performance standards, but shall be given appropriate latitude in how to reach that outcome.

The proposed regulations create a system for review and approval or disapproval of Site Security Plans consistent with this language of Section 550. *See* proposed 27.240. The Department seeks comment on how this proposed process could be improved consistent with the statute.

3. Alternative Security Programs

Section 550 expressly anticipates that covered facilities may prefer to submit Alternative Security Programs (ASP) established by private sector entities, state, or local governments. Pub. L. 109–295, Oct. 4, 2006. Section 550 gives the Secretary discretion to approve such Alternative Security Programs when the Secretary finds that the program meets the requirements of the interim final rule. In the rule text offered below, we define Alternative Security Program as ''a third-party or industry organization program, a state or Federal government program or any element of aspect thereof that the Assistant Secretary has determined provides an equivalent level of security to that established by this subchapter.''

It is possible that an appropriate ASP could be used in part or in whole, including in the place of a Vulnerability Assessment or a Site Security Plan, or both, depending on the nature of the ASP. The Department may choose to approve or disapprove an ASP for a specific covered facility or on a broader scale by approving or disapproving an industry association or government program as an ASP for use in accordance with this rule.

Under the Alternative Security Program provisions in proposed 27.235, the Secretary may specifically designate existing programs, Vulnerability Assessments, and Site Security Plans completed thereunder as satisfactory under Section 550. The Department will begin accepting requests for approval of existing Alternative Security Programs on December 28, 2006. Such requests should be made to the Assistant Secretary. Guidance for such submissions will be made available on the Department's Web site.

4. Guidance Regarding Site Security Plans

Although the Department may not mandate any particular security measure, it may issue guidance specifying what types of measures, if selected, would presumptively satisfy the performance standards. Such guidance would identify options for meeting the standards but would not mandate any particular choice of measures to meet the performance standards. A covered facility would always be permitted to select other measures (whether contemplated by the guidance or not) that could satisfy the performance standards. The Department intends to seek public comment prior to issuance of such guidance to the extent consistent the level of information protection contemplated by the statute.

F. Audits and Inspections

Section 550(e) gives the Department the authority to audit and inspect chemical facilities in order to determine compliance with its requirements. This section imposes an affirmative duty on chemical facilities to cooperate with authorized DHS officials and allow inspections and audits. DHS expects that it will carry out this audit and inspection authority through the Assistant Secretary for Infrastructure Protection and his designees, or for certain lower risk tiers of facilities, through appropriate third party auditors. The Department is considering a program for certain tiers of facilities involving the certification and use of these Third-Party Auditors. *See* proposed § 27.245.

DHS (or, in appropriate cases, a DHS-certified Third-Party auditor) will conduct inspections of each covered facility before issuing final approval for a Site Security Plan. DHS could also conduct audits and inspections outside of the Site Security Plan approval cycle in exigent circumstances. By its terms, this inspection authority extends to all chemical facilities. Although it is possible that a facility could be inspected to determine whether it presents a high security risk under the statute, the proposed rule suggests a different protocol in most cases. *See, e.g.*, proposed 6 CFR 27.200(c).

Generally speaking, DHS will conduct inspections at reasonable times and in a reasonable manner given all of the circumstances surrounding the particular chemical facilities' operations and the threat information that is available to DHS at any given time. Following promulgation of the interim final rule, the Assistant Secretary will issue guidance to those officials and inspectors who will be conducting inspections and will closely monitor the results of such inspections. This ensures that there will be uniformity in inspection procedures and in Departmental enforcement of these regulations.

During inspections of chemical facilities, authorized DHS officials (or third party auditors under certain circumstances) may inspect property or

equipment, view and/or copy records, and audit records and/or operations. DHS expects that it will conduct inspections during regular business hours of 9 a.m. to 5 p.m. DHS will provide facility owners with advance notice of inspections, except where the Under Secretary or Assistant Secretary determines that exigent circumstances preclude notice and personally approves such an inspection. The circumstances leading the Under Secretary or Assistant Secretary to approve an unannounced inspection might include threat information warranting immediate action.

G. Background Checks

A proposed standard on personnel surety would require covered facilities to ''perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or potentially critical targets.'' The Department believes that this component of the security standards will enhance security in what would otherwise be a significant potential vulnerability. In crafting and enforcing this standard, the Department understands that many facilities covered under these regulations already perform background checks on employees and those who have access to the facilities. The Department therefore encourages comment from industry, labor unions, and individuals on their experiences with this subject.

The Department is considering several components of this issue, including the following: (1) The individuals for whom background checks would be conducted (whether that would include employees with access to restricted areas of the facility, all employees, unescorted visitors, all individuals with access to the facility or any combination of the above); (2) The timing of this requirement particularly as it applies to employees (i.e., whether a background check should be conducted in association with the hiring process and, if so, how to address this requirement for current employees); (3) The type of background check that should be conducted and therefore the type of personally identifiable information that would be required of these individuals, such as biometrics. Background checks might include a terrorism name check against the consolidated Terrorist Screening Database, a fingerprint-based check against terrorism and/or criminal history records, or a broader law enforcement or immigration status check; (4) Whether the government should conduct these checks or whether the industry could use authorized third parties to conduct the checks. The Department requests comments on these issues.

In another context, the Department will require background checks for all individuals having access to ''secure areas'' of the maritime transportation system when those individuals are not accompanied by someone who already has a sufficient background check. *See* 46 U.S.C. 70105(a); *see also* 71 FR 29,396 (May 22, 2006) (notice of proposed rulemaking to implement the Transportation Worker Identification Credential (''TWIC'') program in the maritime sector). Would an access restriction such as that in the proposed TWIC program be appropriate in the context of covered chemical facilities? Should any segment of chemical facility personnel participate in TWIC or a similarly structured program? The Department requests comments on these questions.

Second, the Department will consider appropriate grounds for denying access or employment to individuals when their background check reveals an anomaly. In a different context, the Department has developed a list of ''disqualifying crimes,'' as part of a threat assessment process, that prevent individuals from gaining access to certain facilities or privileges. *See* 46 U.S.C. 70105(c); 71 FR 29396 (May 22, 2006) (proposing a list of disqualifying crimes for Hazardous Materials Endorsements (HME) and the Transportation Worker Identification Credential (TWIC) program); *see also* 27 CFR 555.26(c) (ATF prohibited persons criteria). Should the background check standards used in the HME and TWIC contexts apply to chemical facility security programs? (Preliminarily, the Department believes that any person possessing a valid TWIC card would have undergone sufficient background checks for purposes of the Section 550 security standards.)

The Department will consider, as one option, the background check process employed by ATF. *See* 27 CFR 555.33. In this process, licensees submit to ATF the names and identifying information for persons and employees authorized to possess explosive materials in the course of employment. ATF then conducts a background check and provides a ''letter of clearance'' or a written determination that the individual should not hold a position requiring the possession of explosive materials. This process also includes an appeals process. *See* 27 CFR 555.33(b). The Department requests comments on whether this type of process, along with an associated fee charged to facility owners and operators would be appropriate.

H. Approval and Disapproval of Vulnerability Assessments and Site Security Plans

Section 550 states that ''the Secretary shall review and approve each vulnerability assessment and site security plan required under this section.'' *See* Pub. L. 109–295, sec. 550(a). To implement this provision of the statute, and consistent with the implementation plan discussed herein, the Department will require all covered facilities to submit Vulnerability Assessments and Site Security Plans to the Department. The Department will review and approve or disapprove each Vulnerability Assessments in accordance with proposed § 27.215. If the Department approves the Vulnerability Assessment, the Department will issue a letter to the covered facility so stating.

After a review of the Site Security Plan, the Department will preliminarily approve it or disapprove it. In the case of a preliminary approval, the Department will issue a Letter of Authorization to the covered facility. After preliminarily approving a Site Security Plan, the Department will inspect each facility in order to determine compliance with the requirements of this part. (The inspection provisions are discussed more fully above). After issuing a Letter of Authorization, the Department will schedule an inspection of the facility. After the inspection, if the Department concludes that the Site Security Plan addresses the vulnerabilities identified in the Vulnerability Assessment, satisfies the risk-based performance standards, and has been satisfactorily implemented, the Department will issue a Letter of Approval to the covered facility.

If a Vulnerability Assessment or Site Security Plan fails to satisfy the specified, ''risk-based performance standards,'' the Department will disapprove the relevant document. *See* Pub. L. 109–295, Sec. 550(a) (''the Secretary may disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established by this section''). If the Department concludes that the Site Security Plan has not been satisfactorily implemented, the Department will consult with the covered facility as provided in proposed 27.240(b) and schedule a second inspection.

When disapproving the Vulnerability Assessment or Site Security Plan, the Department will provide the facility with a written explanation as to why the

Department disapproved the assessment or plan. Taking into account the nature of the facility and other relevant circumstances, the Department will also specify a date by which the facility must provide to the Department a modified Vulnerability Assessment or Site Security Plan. If a facility fails to provide an acceptable Vulnerability Assessment or Site Security Plan by the specified date, the Department may issue an Order Assessing Civil Penalty under proposed § 27.305.

As with other elements of implementing Section 550, however, the implementation of the receipt, review, and approval of Vulnerability Assessments and Site Security Plans will proceed in a phased approach based on the tiering of covered facilities. *See* proposed § 27.230. The Department will provide covered facilities with a schedule identifying timing requirements for submitting and updating Vulnerability Assessments and Site Security Plans under proposed §§ 27.215 and 27.225, as well as the timing, frequency, and nature of the inspections required under proposed § 27.245.

Facilities in Tier One must submit Vulnerability Assessments to the Department within 60 calendar days. These facilities must submit Site Security Plans within 120 calendar days.

The Department will also require that covered facilities update or renew their Vulnerability Assessments and Site Security Plans on a regular basis or as needed basis. The timing for this requirement will also depend upon the tiering of covered facilities. In general, the Department believes that Tier One facilities should update and renew their Vulnerability Assessments and Site Security Plans each year; Tier two facilities should update and renew their Vulnerability Assessments and Site Security Plans on two-year cycles; and any additional tiers should update and renew their Vulnerability Assessments and Site Security Plans on three-year cycles. For individual facilities, and based on information concerning those particular facilities, the Department may determine that more or less frequent update and renewal cycles are appropriate. The Department seeks comment on this strategy for updating and renewing vulnerability assessments and site security plans.

I. Remedies

The proposed regulation specifies the remedies that the Department can use to achieve compliance with the requirements of this part. At the most basic level, the Department can issue an Order for Compliance pursuant to proposed § 27.300. The Assistant Secretary may issue such an Order for any instance of noncompliance, such as a chemical facility's refusal to complete a Top-screen, failure to allow DHS to conduct an inspection, or failure to update a Site Security Plan.

Where the Department finds that there is a repeated pattern of noncompliance or egregious instances of noncompliance with the requirements of this part, the Department may issue civil penalties of not more than $25,000 for each day during which the violation continues (*see* 550(d) and 49 U.S.C. 70119(a)) and/or order chemical facilities to cease operations (*see* section 550(g)). The Department considers the cease operations order to be an extraordinary authority and would use it only so along as other remedial provisions hereunder could not achieve compliance.

The proposed requirements in § 27.305 and § 27.310 specify the methods by which DHS will issue civil penalties and cease operation orders. Proposed § 27.315 outlines general requirements that apply to all orders, including orders for compliance, assessing civil penalty, and to cease operations. Of note, the proposed regulation provides that all of these orders are inoperative while an appeal is pending under § 27.320 and that an order issued under this subpart does not constitute final agency action until a chemical facility exhausts all appeals or the time for such appeals has lapsed. Chemical facilities must exhaust all appeals specified in this regulation before pursuing an action in Federal District Court. As noted, the Department recognizes that an Order to Cease Operations would likely be litigated immediately after issuance. This authority would be utilized when no other options will achieve the required result. At the same time, the Department recognizes the necessity and importance of these tools to foster incentives for compliance.

Finally, as the Department indicates in the proposed regulation, DHS may issue appropriate guidance and necessary forms for the issuance of Orders under this subpart. Such guidance might include procedures for, notifications made, and meetings conducted pursuant to §§ 27.300, 27.305, 27.310, and 27.315.

In using these administrative remedies, the Department has sought to include several opportunities for review of Departmental decisions, including opportunities for chemical facilities to consult with the Department, to present additional evidence, to defend against any alleged violations, and to explain its efforts to rectify alleged violations. The Department recognizes that these are powerful tools and accordingly wants to ensure that there are sufficient mechanisms in place for facilities to respond to the use of these tools. The Department seeks comment on its proposed requirements for the use of these administrative remedies.

J. Objections and Appeals

This rule proposes to provide chemical facilities with various opportunities throughout the process to object to a Departmental decision. The Department intends for the process to be as simple and quick as possible but recognizes that the review needs to be meaningful. The proposed rule provides chemical facilities with two mechanisms with which to challenge a Departmental decision, an objection and an appeal.

The basic mechanism is called an ''objection.'' A chemical facility may object to (1) a determination that the facility presents a high level of security risk, (2) its placement in a risk-based tier, and/or (3) a disapproval of its Site Security Plan. To do so, a chemical facility must file an objection according to the procedures specified in the pertinent section—either 6 CFR 27.205(c) ''Determination that a Chemical Facility Presents a High Level of Security Risk—Objection,'' 6 CFR 27.220(b) ''Tiering—Objection,'' or 6 CFR 27.240(c) ''Review and Approval of Vulnerability Assessments and Site Security Plans—Objection to Disapproval of Site Security Plan.'' Under the scheme for these proposed regulatory provisions, a chemical facility files an Objection and may request a meeting, and the objection could be addressed in as few as 20 days.

The other review mechanism available to chemical facilities is an appeal. The Department recognizes that certain matters, such as a final determination disapproving a Site Security Plan or the issuance of an Order, can be of significant consequence. As a result, these matters require a more lengthy review. To that end, the Department is proposing to provide chemical facilities with an opportunity to appeal any Order issued under this regulation and any determination disapproving a Site Security Plan. Proposed § 27.320(a)(1) and (2) allows chemical facilities to appeal to the Under Secretary and General Counsel for Site Security Plan disapprovals and all Orders except Orders to Cease Operations. Proposed § 27.320(a)(3) allows chemical facilities to appeal to the Deputy Secretary for Orders to Cease Operations. The

adjudicating official may then affirm, revoke, or suspend a determination or Order.

Also of note in this section, any decision made by an adjudicating official under § 27.320(c) of this section constitutes final agency action. In addition, the failure of a chemical facility to file an appeal in accordance with the procedures and time limits contained in this section results in the Assistant Secretary's determination or issuance of an Order becoming final agency action. Finally, a chemical facility will need to exhaust the appeal processes specified in these regulatory provisions before pursuing an action in Federal District Court. The Department requests comment on the proposed process for objections specified in § 27.205(c), § 27.220(b), § 27.240(c), and § 27.320, including comment on specific provisions in the process and the adequacy of these procedures generally.

K. Chemical-Terrorism Vulnerability Information

Section 550(c) of the Homeland Security Appropriations Act of 2007 provides the Department with the authority to protect from inappropriate public disclosure any information developed pursuant to Section 550, ''including vulnerability assessments, site security plans, and other security related information, records, and documents.'' In considering this issue, the Department recognized that there are strong reasons to avoid the unnecessary proliferation of new categories of sensitive but unclassified information, consistent with the President's Memorandum for the Heads of Executive Departments and Agencies of December 16, 2005, entitled ''Guidelines and Requirements in Support of the Information Sharing Environment.'' With Section 550(c), however, Congress acknowledged the national security risks posed by releasing information relating to the security and/or vulnerability of high risk chemical facilities to the public generally. For all information generated under the chemical security program established under Section 550, Congress gave the Department broad discretion to employ its expertise in protecting sensitive security and vulnerability information. Accordingly, the Department proposes herein a category of information for certain chemical security information called Chemical-terrorism Security and Vulnerability Information (CVI).

Congress also recognized that, to further the national security interests addressed by Section 550, the Department must be able to vigorously enforce the requirements of Section 550, and that these efforts may include the initiation of proceedings in federal district court. At the same time, it is essential that any such proceedings not be conducted in such a way as to compromise the Department's ability to safeguard CVI from public disclosure. For this reason, Congress provided that, in the context of litigation, the Department should protect CVI more like Classified National Security Information than like other sensitive unclassified information. This aspect of Section 550(c) has no analog in other sensitive unclassified information regimes.

1. Protection From Public Disclosure

In setting forth the minimum level of security the Department must provide to CVI, Section 550(c) refers to 46 U.S.C. 70103, which was enacted by the Maritime Transportation Security Act of 2002: ''Notwithstanding any other provision of law and subsection (b), information developed under this section * * * shall be given protections from public disclosure *consistent with similar information developed by chemical facilities subject to regulation under section 70103 of* title 46, United States Code.'' (Emphasis supplied.) Section 70103(d) provides that ''information developed under this chapter [pertaining to Port Security] is not required to be disclosed to the public.'' As discussed below, by regulations existing at the time Congress enacted Section 550, security plans issued pursuant to 46 U.S.C. 70103 constitute Sensitive Security Information (SSI), the public disclosure of which is heavily regulated. *See* 49 CFR 1520.5(b)(2)(ii). It is the Department's view that by requiring the Department's handling of CVI to be ''consistent with'' information covered under 46 U.S.C. 70103, Congress intended CVI to receive a level of security not inconsistent with that provided to SSI. Yet the Department also believes that Section 550(c) provides the Department with broad discretion and maximum flexibility to employ more rigorous standards to protect CVI from inappropriate public disclosure as necessary. Furthermore, Section 550(c) provides specifically that ''in any proceeding to enforce this section, * * * information submitted to or obtained by the Secretary, and related vulnerability or security information, shall be treated as if the information were classified material.''

Section 114(s) of title 49 of the U.S. Code requires TSA to promulgate regulations governing the protection of certain sensitive unclassified information, including information that would ''be detrimental to the security of transportation'' if publicly disclosed. 49 U.S.C. 114(s). In response, TSA issued, 49 CFR part 1520, which establishes certain requirements for the recognition, identification, handling, and dissemination of Sensitive Security Information or ''SSI,'' including restrictions on disclosure and civil penalties for violations of those restrictions. Under the regulations, SSI includes any security programs issued, established, required, received or approved by the Department of Transportation or the Department. These include any vessel, maritime facility or port area security plan required by Federal law and any national or area security plan prepared pursuant to 46 U.S.C. 70103. In addition, SSI includes selection criteria used in security screening processes, Security Directives and Information Circulars, threat information and vulnerability assessments concerning transportation facilities, and technical specifications of security screening and detection systems and devices.

Access to SSI is strictly limited to those persons with a need to know, as defined in 49 CFR 1520.11, and to those persons to whom TSA makes a specific disclosure authorization under 49 CFR § 1520.15. In general, a person has a need to know specific SSI when he or she requires access to the information: (1) To carry out transportation security activities that are government-approved, -accepted, -funded, -recommended, or -directed, including for purposes of training on, and supervision of, such activities; (2) to provide legal or technical advice to airport operators, air carriers or their employees regarding security-related requirements; or (3) to represent covered persons in judicial or administrative proceedings regarding security-related requirements. Individuals with a need to know or to whom SSI is disclosed pursuant to § 1520.15, including in the context of an administrative enforcement proceeding, may, at TSA or Coast Guard's discretion, be required to satisfactorily complete a security background check to gain access to SSI. Civil litigants do not have a regulatory need to know, unless they fall into the categories noted above.

The SSI regulations also set forth restrictions on the disclosure of SSI. These restrictions apply to individuals and entities with a need to know as well as others deemed by 49 CFR 1520.7 to be ''covered persons.'' The restrictions, which are set forth in 49 CFR 1520.9, include a duty to protect information by, among other things, only disclosing or providing access to SSI to covered

persons with a need to know and storing SSI in a secured container. Section 1520.9 also requires any covered person to promptly report to TSA or other applicable agency any unauthorized disclosure of SSI. As part of the Homeland Security Appropriations Act of 2007, Congress gave TSA the authority to assess a civil penalty of up to $50,000 for each violation of 49 CFR part 1520 by a person provided access to SSI under Section 525(d).

Congress has long authorized the protection of sensitive unclassified information in the context of nuclear facilities. *See* 42 U.S.C. 2167, 2168 (authorizing Nuclear Regulatory Commission (NRC) to issue regulations and civil and criminal penalties, protecting safeguards information or ''SGI'' from inadvertent release and unauthorized disclosure that might compromise security of nuclear facilities or materials); *see also* 10 CFR 73.21 (defining SGI to include ''security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities''); § 73.21(c) (authorizing access to SGI where both valid ''need to know'' information and authorization based on an appropriate background investigation under 10 CFR part 73); § 73.21(d) (setting forth physical protection requirements). And Congress authorized a similar regime more recently to protect voluntarily submitted critical infrastructure information as part of the Homeland Security Act of 2002. *See* 6 U.S.C. 131 *et seq.*; *see also* 6 CFR 29.4 (describing Protected Critical Infrastructure Information (PCII) program); § 29.7 (requiring background checks for access to PCII and setting forth protection guidelines for handling of PCII); § 29.8 (prohibiting disclosure of PCII except in limited circumstances).

In designing a regulatory scheme to govern disclosure of CVI, the Department has considered the laws regulating SSI, SGI, and PCII. The Department believes that by specifying 46 U.S.C. 70103, Congress provided an avenue to embrace many of the fundamental elements of SSI, except that Congress was more explicit as to the use of information in legal proceedings. Accordingly, the Department proposes that, except as provided below in connection with administrative and judicial proceedings, CVI should be treated in a manner similar to SSI. The Secretary shall administer this Section consistent with section 550, including appropriate sharing with State and local officials, law enforcement officials, and first responders.

2. Protection From Disclosure in Litigation

Section 550(c) provides that ''in any proceeding to enforce this section, * * * information submitted to or obtained by the Secretary, and related vulnerability or security information, shall be treated as if the information were classified material.'' By segregating this information for separate treatment under the statute, Congress sought to provide significant protection for CVI in the course of enforcement proceedings.

Classified information is disclosed in litigation only under extraordinary circumstances. Executive Order 13292, Further Amendment of Executive Order 12958, as Amended, Classified National Security Information, defines ''classified national security information'' or ''classified information'' as ''information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified statutes when in documentary form.'' E.O. 12958 § 6.1(h). More specifically, information may be classified if, among other things, the original classification authority determines that ''the unauthorized disclosure of the information reasonably could be expected to result in damage to national security, which include defense against transnational terrorism, and the original classification authority is able to identify and describe the damage.'' E.O. 13292 § 1.1(a)(4).

By statute, Congress has defined classified information more broadly in certain contexts. The Classified Information Procedures Act (CIPA), which sets forth the proper handling for disclosure of classified information in criminal proceedings, defines classified information as ''any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954.'' 18 U.S.C. App. 3 sec. 1(a). The same definition is used in civil proceedings involving charges of providing material support or resources to designated foreign terrorist organizations. 18 U.S.C. 2339B(g)(1) (''the term 'classified information' has the meaning given that term in section 1(a) of [CIPA]'').

Under section 2339B, where a party seeks classified information in discovery, the court may authorize one of the following as a substitute upon a sufficient *ex parte* showing by the Government: (1) A redacted version of the classified documents; (2) a summary of the information contained in the classified documents; or (3) a statement admitting relevant facts that the classified documents would tend to prove. 18 U.S.C. 2339B(f)(1)(A). Section 2339B also provides protections against the disclosure of classified information through witness testimony. Upon a Government objection, the court will consider an *ex parte* proffer by the Government on what the witness is likely to say and a proffer from the defendant of the nature of the information the defendant seeks to elicit. *Id.* at 2339B(f)(3). If the court denies any such requests by the Government, the Government can take an immediate, expedited interlocutory appeal. *Id.* at 2339B(f)(1)(C), (5). Notably, section 2339B states that it does not prevent the Government from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information, including the invocation of the military and State secrets privilege. *Id.* at 2339B(f)(6).

The procedures set forth in CIPA are substantially similar to those in section 2339B. One notable difference is that the Government may submit to the court an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information. 18 U.S.C. App. sec. 6(c)(2). Where the Government has filed such an affidavit but the court concludes that there is no adequate substitute for the classified information sought by the defendant, the court may dismiss the Government's indictment or information, or order something in lieu of complete dismissal such as dismissing or finding for the defendant only with respect to certain counts. *Id.* at 6(e).

As stated above, Section 550(c) provides only that, in the course of proceedings under section 550, CVI ''shall be treated as if the information were classified material.'' Section 550(c) does not specify to which procedure/s governing the handling of classified material the Department should look—i.e., ordinary civil litigation procedures, civil procedures under section 2339B, criminal procedures under CIPA, or some other regime. The Department is considering alternatives and proposes here that in the context of judicial or administrative enforcement proceedings, the disclosure of CVI shall be governed by the procedures set forth

in section 2339B. Furthermore, to accommodate the possible presence of a jury or any other individuals that are deemed necessary to such proceedings, the Department will retain discretion to authorize access to CVI for persons necessary for the conduct of enforcement proceedings, provided that no one that the Department has not so authorized shall have access to or be present for the disclosure of such information. This has the effect of requiring a court to close the courtroom where CVI is to be revealed, which the Department believes is consistent with Congress's intent that CVI be treated as classified information. Because the Department believes that Section 550(c) cannot reasonably be read to prohibit a chemical facility and its counsel or other relevant employees from gaining access to CVI concerning their own facility for use in enforcement proceedings, the proposed provisions do not apply to such individuals.

For civil litigation unrelated to the enforcement of Section 550, except as provided otherwise at the sole discretion of the Secretary, access to CVI shall not be available. The Department believes that by carefully drafting Section 550(c), Congress did not envision providing access to CVI to third-parties in civil litigation or in any civil litigation not involving enforcement of Section 550. As discussed above, Section 550(c) requires very restrictive handling of CVI in enforcement proceedings, *i.e.*, handling at least consistent with the handling of classified information. We believe that Congress could not have intended the Department to afford CVI lesser protection in the context of civil litigation, especially where the litigation is unrelated to the enforcement of Section 550. The level of protection for CVI in civil litigation proposed herein is not inconsistent with the regime governing SSI prior to the Homeland Security Appropriations Act of 2007. The Department believes, however, that, in light of amendments to the SSI regime contained in section 525(d) of the Homeland Security Appropriations Act of 2007, to give full effect to Section 550(c), the Department must provide expressly for the prohibition on disclosure of CVI in civil litigation. Among other things, section 525(d) granted civil litigants who do not have a regulatory need to know access to specific SSI in federal district court proceedings, if certain requirements are met. Moreover, the Department believes that the proposed prohibition is consistent with the ordinary handling of classified information in civil proceedings, access to which may be ordered only in a narrow class of cases and under extraordinary circumstances.

The Department seeks comment on whether an alterative to the approach described herein is more desirable. Other alternatives may include handling CVI in proceedings in the same manner as SSI or some other category of sensitive unclassified information, or as classified information under CIPA.

L. Statutory Exemptions

Section 550 exempts from its coverage several categories of facilities. According to the statutory exemptions, the regulations issued under Section 550 will not apply to public water systems (as defined by section 1401 of the Safe Drinking Water Act); water treatment works facilities (as defined by section 212 of the Federal Water Pollution Control Act); any facilities owned or operated by the Departments of Defense and Energy; and any facilities subject to regulation by the Nuclear Regulatory Commission. The regulations promulgated under Section 550 also will not apply to maritime facilities regulated by the Coast Guard pursuant to the Maritime Transportation Security Act of 2002. These facilities will not need to submit information to the Department under the Section 550 regulations. The Department, however, is considering how to apply this rule to those facilities that are not subject to the security standards of part 105 of the maritime security regulations but may be covered by other maritime security regulations pursuant to the Maritime Transportation Security Act of 2002. The Department seeks comment on the applicability of this rule to such facilities.

Section 550 also provides that ''[n]othing in this section shall be construed to supersede, amend, alter, or affect any Federal law that regulates the manufacture, distribution in commerce, use, sale, other treatment, or disposal of chemical substances or mixtures.'' ATF regulates the purchase, possession, storage, and transportation of explosives. The Department does not intend for the regulations issued under Section 550 to impede ATF's current authorities. Where there is concurrent jurisdiction, the Department will work closely with ATF to ensure that the regulated entities can comply with the applicable regulations while minimizing any duplicative efforts by such entities.

III. Implementation

A. Immediate Priority on Highest Risk Facilities

The Department is considering a ''phased'' implementation of its Section 550 program. Phase I would begin immediately following promulgation of the interim final rule in April 2007 and would focus on a selected number of chemical facilities identified from data in the RMP program and other sources as potentially posing the most significant risk to neighboring populations. The Assistant Secretary would contact each of these chemical facilities directly and request that each complete the Top-screen process within a reasonable but relatively brief period. Technical assistance with the Top-screen Process would be provided immediately to any chemical facility in this group so that progress could be achieved on an accelerated schedule. Shortly after receipt of the completed Top-screen information, the Assistant Secretary would notify each of these facilities pursuant to proposed § 27.205 (regarding whether it qualifies as ''high risk'' and its initial placement in a risk-based tier). For each high risk, or ''covered,'' facility, the Assistant Secretary would provide a schedule for submission of its Vulnerability Assessment and Site Security Plans under § 27.210 of the proposed regulations. The Department's initial emphasis would be on the highest risk facilities in this group and the Department would prioritize reviews of those chemical facilities by risk, and it would schedule submissions accordingly. Again, the chemical facilities in this Phase 1 group could request and receive technical assistance in completing these processes.

Upon receipt, submissions of Vulnerability Assessments and Site Security Plans for Phase 1 covered facilities would be subject immediately to review under § 27.240 of the proposed regulations, and notified as soon as possible if additional submissions or revisions are necessary and, if not, of the results of such reviews. Again, where consultation or revisions would be necessary to bring the submissions into compliance, the process under §§ 27.215 and 27.225 would be available for that purpose. Following approval of the Vulnerability Assessment and Site Security Plan, the Department would contact the covered facility to arrange for an appropriate schedule for a compliance review inspection and audit.

While Phase 1 is underway, the Assistant Secretary would also initiate a broader Phase 2 process. For Phase 2,

the Assistant Secretary would, under § 27.200 of the proposed regulations, publish criteria identifying an additional group or type of facilities that should complete the Top-screen process. The Assistant Secretary could also contact facilities directly and request completion of the Top-screen under § 27.200 of the proposed regulations as appropriate. Phase 2 would then progress under the proposed regulations under the standard timeframes contemplated by those regulations. When appropriate, the Assistant Secretary would prioritize and could expedite review for a particular covered facility based on risk.

Finally, as Phase 2 is underway, the Assistant Secretary could, as soon as appropriate, initiate a Phase 3 process for other high risk facilities not addressed in Phases 1 and 2. We contemplate that Phase 1 would be completed as soon as possible, and certainly during the first year of the program. Phase 2 would be well underway during year one, but could be completed during the second year. Phase 3 could begin some time later. Of course, every covered facility in each of these 3 proposed program phases would be subject to requirements of §§ 27.215, 27.225, and 27.245 for continuing obligations for plan updates, audits and inspections. Pursuant to § 27.215 and § 27.225 of the proposed rules, the frequency and nature of these continuing requirements would vary for covered facilities based on placement in the risk-based tiers.

If such a phased system is implemented, the Department would issue guidance further describing each phase in additional detail.

The Department requests comment on the viability and practicality of this phasing proposal for the Section 550 program.

B. Consultations and Technical Assistance

As with any new regulatory program, it is very important that the Department ensure a uniform and fair approach in each of the programmatic phases to the many activities described in these regulations. Uniformity could be particularly difficult to achieve as the program matures, as new officers are trained and begin the process of reviewing Vulnerability Assessments and Site Security Plans, and as audits and inspections are conducted. The Department has several structural means to address its concerns about uniformity and fairness. First, at each step of the process, a facility may seek to ''consult'' with Department officials on procedural or policy matters or on the application of the performance standards. Such consultations are addressed in section § 27.115 of the proposed regulations. Second, the Assistant Secretary and a designated Coordinating Official will have a specific responsibility under these regulations to ensure uniformity and fairness by program officials. Third, to the extent that resources permit, the Department will provide technical assistance to covered facilities. As the program matures and further guidance is issued, the level of necessary technical assistance may decline. But in the initial stages of the program, this type of assistance may be very important. The Department recognizes that the initial period of the program implementation will be the most challenging for covered facilities. The Department requests comment on these and other activities that may improve the implementation process. Note also that the proposed regulations also contemplate more formal processes for administrative Objections and Appeals in sections 27.205(c); 27.220(b); 27.240(b), (c); 27.310(c); and 27.320.

IV. Other Issues

A. Third-Party Lawsuits

Section 550 provides that ''nothing in [that] section confers upon any person except the Secretary a right of action against an owner or operator of a chemical facility to enforce any provision of this section.'' Pub. L. 109–295, Sec. 550. Proposed § 27.410 codifies that provision in the regulations. The Department believes that this statutory and regulatory language prohibits any effort by a State or local government or other third party litigant to enforce the provisions of Section 550, or to compel the Department to take a specific action to enforce Section 550. Thus, the Department has discretion to determine when and how to enforce. Note also that Section 550 has strict information protection provisions for the type of security information that would be critical to any enforcement matter: ''That in any proceeding to enforce this section, vulnerability assessments, site security plans, and other information submitted to or obtained by the Secretary under this Section, shall be treated as if the information were classified material.'' Pub. L. 109–295, Sec. 550(c).

B. Application to Facilities Manufacturing and/or Storing Ammonium Nitrate

Section 550 provides authority for the Department to regulate ''chemical facilities'' without restricting that authority to facilities manufacturing or storing any particular type of chemical substance. The Department is aware, however, that some legislative proposals not yet enacted into law contain specific provisions regarding the security measures associated with ammonium nitrate. See H.R. 3197, 109th Cong. (2006), S. 2145, 109th Cong. (2006). The Department currently plans to treat ammonium nitrate chemical facilities in the same manner that it treats facilities with other chemicals: whether the regulations govern a particular ammonium nitrate chemical facility will depend upon the nature of the facility and the risk assessment results. The Department seeks comments, however, on the application of the proposed regulations to ammonium nitrate chemical facilities.

C. Regulatory Requirements/Matters

1. Executive Order 12,866

Executive Order 12,866, Regulatory Planning and Review, requires an assessment of the potential costs and benefits of regulatory actions. When the Department publishes the interim final rule, we will include our analysis of the expected costs of the regulation and an assessment of the benefits of the regulation. Interested persons are invited to provide comment on all aspects of the potential costs and benefits in order to assist the Department with its analysis. Comments containing trade secrets, confidential commercial or financial information, or SSI should be appropriately marked and submitted in accordance with the procedures explained above in the **ADDRESSES** section. Comments that will provide the most assistance to the Department with this rulemaking include, but are not limited to:

- The economic impact (both long-term and short-term, quantifiable and qualitative) of the implementation of Section 550.
- The monetary and other costs anticipated to be incurred by facility owners and/or operators and any distributional effects on U.S. citizens.
- The benefits of the rulemaking.

In order to help facilitate meaningful public comment, the Department would like to set forth a potential methodology for analyzing the costs of the interim final rule. We have reviewed the methodology used by the Coast Guard to analyze the economic impact of the 33 CFR part 105 Facility Security final rule, and, due to the similarities between the two rules, believe that this methodology has merit and should be considered for application in this rulemaking. The MTSA Facility Security final rule, at 68

FR 60536 (Oct. 22, 2003), estimated the cost of performance standards on several thousand unique facilities. Similarly, the interim final rule will estimate the costs of risk-based performance standards to possibly several thousand unique facilities. The Coast Guard found it impractical to attempt to estimate compliance costs for each individual facility and instead developed costs based on 16 ''model facilities.'' Each of the several thousand facilities was placed into one of the 16 different subgroups for which compliance costs were then estimated. Once the compliance costs for the 16 ''model facilities'' were calculated, estimating the cost of the regulation was relatively straightforward.

For the cost assessment which will accompany the interim final rule, the Department may estimate compliance costs based on the ''model facility'' concept explained above. Even though the interim final rule will utilize risk based performance standards and facilities will have discretion on how to meet the performance objectives, the cost assessment will need to make broad assumptions regarding the percentage of facilities that will choose to implement or continue certain security measures for the purposes of estimating compliance costs. For example, many facility owners and/or operators will choose to build or improve fences, enhance perimeter lighting, and hire additional security guards and we may need to make assumptions on how facilities will choose to implement the security measure in order to calculate an estimated cost. The Department is requesting public comment on how best to group facilities that will need to comply with this interim final rule into ''model facilities'' for cost estimating purposes, and we are especially interested in public comment on the criteria presented below:

- Should the ''model facility'' criteria incorporate risk-based tiering? Compliance costs may differ for a facility according to its risk-based tier.
- Should the ''model facility'' criteria consider the size of the facility? Larger facilities may face higher compliance costs than smaller facilities as larger facilities may need to construct longer fences or hire more guards. For the purpose of facilitating comment, we will assume that facilities with six or more chemical processes or chemicals being stored or used would be considered to be ''larger.''
- Should facilities that are enclosed (i.e., warehouses, enclosed manufacturing sites) be treated as a ''model facility'' for cost estimating purposes?
- Should facilities that might be targeted by criminals for chemical theft or diversion be treated as a ''model facility'' for cost estimating purposes?
- The ''model facility'' estimates are expected to include current market prices of possible security enhancements that facilities may choose to undertake. Possible enhancements include, but are not limited to: Primary and secondary fences, barriers at the gate, perimeter vehicle barrier, perimeter lighting, inside lighting, CCTV system, guards, guards houses, fence line intrusion detection system, handheld radios, staging area for vehicle screenings and enhanced communication systems. The Department is requesting information that will assist with the estimation of these and any other security enhancements. We have placed an estimate of the capital costs of specific security enhancements in the docket in order to facilitate public comment.

2. Regulatory Flexibility Act

DHS has not assessed whether this rule will have a significant economic impact on a substantial number of small entities, as defined in the Regulatory Flexibility Act (5 U.S.C. 601–612). The term ''small entities'' comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. Under Executive Order 13,272 and the Regulatory Flexibility Act, when an agency publishes a rulemaking without prior notice and opportunity for comment, the Regulatory Flexibility Act requirements do not apply. This rule does not require a general notice of proposed rulemaking and, therefore, is exempt from the requirements of the Regulatory Flexibility Act. Although this rule is exempt, we request comment on the economic impact of this rule on small entities.

3. Executive Order 13,132: Federalism

The regulations issued under Section 550 have the potential to affect current or future State laws and regulations. Although few States currently regulate chemical facilities as a means to prevent or mitigate terrorist attacks, the Department plans to consult with State officials, to the extent practicable, prior to promulgating the interim final rule. *See* Exec. Order No. 13,132, 64 FR 43255 (Aug. 10, 1999). The Department also encourages State and local officials to provide comments in response to this advance notice. The Department specifically seeks comment on the interaction of the proposed regulations with existing State and local laws and regulations. As discussed in more detail below, the Department has particular interest in considering the effects of State and local laws and regulations on the security-related purposes of Section 550 and the proposed regulations.

The security of the Nation's chemical facilities is a matter of national and homeland security. Remarks of Secretary Michael Chertoff, March 21, 2006, and Sept. 8, 2006. As such, it is the Federal government, and specifically the Department of Homeland Security, that takes on the lead and coordinating role. Among the primary missions of the Department are the prevention of terrorist attacks within the United States; the reduction of the vulnerability of the United States to terrorism; and the responsibility to ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland. 6 U.S.C. 111. These aims are necessarily national in scope, and the regulations designed to enhance the security of chemical facilities against terrorist attack reflect a considered judgment concerning the Department's core mission. State and local governments may also take on a vital role, particularly as first responders and in other response capacities, but the threat of terrorist attacks, which often involve interstate and international activities, remains a significant national threat.

Federal preemption doctrines are founded on the Supremacy Clause of the U.S. Constitution. U.S. Const. art. VI, cl. 2. The law of preemption recognizes that state laws must give way to Federal statutes and regulatory programs to ensure a unified and coherent national approach in areas where the Federal interests prevail—such as national security. *See Crosby* v. *National Foreign Trade Council*, 530 U.S. 363, 375–76 (2000).

Preemption can be expressly set forth in a statute or regulation, or implied by law. The nature of express preemption depends on the language of the statute or regulation that preempts state law. Express preemption language in prior legislative proposals on chemical security was controversial. Preemption language in certain legislative proposals was criticized as far too narrow, expressly allowing a patchwork of inconsistent or contradictory state or local security regulations that would compromise a uniform effective Federal program. Language in other legislative proposals was criticized as too broad, potentially preempting state regulatory efforts at chemical facilities for

environmental, workplace safety and other non-security purposes.

Ultimately, Section 550 was silent on preemption. Cong. Rec. H7968–69 (daily ed. Sept. 29, 2006) (statement of Chmn. Barton) (''During negotiations it was discussed and consciously decided among the authorizing committee negotiators to not include a provision exempting this section from Federal preemption because we do not want a patchwork of chemical facilities that are trying to secure themselves against threats of terrorism caught in a bind of wondering whether their site security complies with all law.''). Thus, the question of Federal preemption will turn either on the application of implied preemption, or on the nature of any express preemption in the Department's regulations.

The application of implied preemption usually turns on the principle that no state or local authority can frustrate the purposes of a Federal law or regulatory program. In reviewing implied preemption questions, Federal courts typically ask whether the state measure poses an ''obstacle'' to the federal law or regulatory regime, or would ''frustrate the purposes'' of the Federal regulatory program. *See Geier*, 529 U.S. at 873; *Hines* v. *Davidowitz*, 312 U.S. 52, 67 (1941); *cf. United States* v. *Locke*, 529 U.S. 89 (2000).

Federal preemption questions can arise both in the courts' application of state common law—often state tort law—or in the application of a state statute or state or local regulation, ordinance or similar measure. In a state tort suit, the question may be whether imposing liability for particular activities would be consistent or inconsistent with Federal law or a Federal regulatory program. For instance, how could state tort law impose liability for actions specifically approved under a Federal program? *See Geier* v. *American Honda Motor Co.*, 529 U.S. 861, 882 (2000); *Colacicco* v. *Apotex, Inc.*, 432 F. Supp. 2d 514 (E.D. Pa. 2006). For a state or local regulation, the question will often be whether the state measure would require activity that could interfere with, hinder or frustrate the Federal program. *Jones* v. *Rath Packing Co.*, 430 U.S. 519, 525–26 (1977); *Geier*, 529 U.S. at 873. A state or local regulation may be preempted, for example, where that regulation conflicts with an activity or plan specifically approved under Federal law.

Section 550 preempts State laws and laws of their political subdivisions that conflict with the regulations promulgated thereunder. *See, e.g., Fidelity Fed. Sav. & Loan Ass'n* v. *De la Cuesta*, 458 U.S. 141, 153 (1982) (''Federal regulations have no less pre-emptive effect than federal statutes.''); *id.* at 154 (a ''pre-emptive regulation's force does not depend on express congressional authorization to displace state law'').

In Section 550, Congress created a carefully balanced regulatory relationship between the Federal government and chemical facilities. Section 550 instructs the Department to establish risk-based performance standards for facility security and the statute allows the Department to disapprove any site security plan that does not meet those standards. Pub. L. 109–295, Sec. 550 (''the Secretary may disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established by this section''). But Section 550 also compels the Department to preserve chemical facilities' flexibility to choose security measures to reach the appropriate security outcome. *Id.* (''regulations [issued under this statute] shall permit each such facility, in developing and implementing site security plans, to select layered security measures that, in combination, appropriately address the vulnerability assessment and the risk-based performance standards for security for the facility''). A state measure frustrating this balance will be preempted.

The proposed regulatory text in section 27.405(a) below recognizes this balance and provides that: ''No law or regulation of a State or political subdivision thereof, nor any decision rendered by a court under state law, shall have any effect if such law, regulation, or decision conflicts with, hinders, poses an obstacle to or frustrates the purposes of these regulations or of any approval, disapproval or order issued thereunder.'' The Department is particularly concerned that a conflict or potential conflict between an approved Site Security Plan and state regulatory efforts could create ambiguity that would delay or compromise implementation of security measures at a facility. To avoid any such delays, there may be an immediate need to address potential preemption and clarify application of the law. To meet this need, the proposed regulations, at § 27.405, would permit State or local governments, and/or covered facilities, to seek opinions on preemption from the Department. Such a process has been used by Congress in other contexts, *see, e.g.*, 49 U.S.C. 31141 (review and preemption of State laws and regulations addressing motor vehicle safety). In most cases, the Department would utilize the process to address quickly a specific conflict between a particular application of state law or local law and an approved site security plan or other elements of the Section 550 program. Note that the Department has the authority to make preemption determinations as it administers the chemical security program under Section 550. *See* Brief of the United States as *Amicus Curiae* at 26, *Watters* v. *Wachovia Bank, N.A.*, 2006 WL 3203255, 126 S.Ct. 2900 (2006) (No. 05–1342) (filed Nov. 3, 2006) (''When an agency concludes, in an exercise of delegated *policymaking* authority, that displacement of state law is warranted in furtherance of a federal statute that it is entrusted to administer, the agency is acting within the core of its expertise.'')

4. Unfunded Mandates Reform Act Assessment

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), enacted as Pub. L. 104–4 on March 22, 1995, requires each Federal agency, to the extent permitted by law, to prepare a written assessment of the effects of any Federal mandate in a proposed or final agency rule that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any one year. Section 204(a) of UMRA, 2 U.S.C. 1534(a), requires the Federal agency to develop an effective process to permit timely input by elected officers (or their designees) of State, local, and tribal governments on a proposed ''significant intergovernmental mandate.'' A ''significant intergovernmental mandate'' under the UMRA is any provision in a Federal agency regulation that will impose an enforceable duty upon State, local, and tribal governments, in the aggregate, of $100 million (adjusted annually for inflation) in any one year. Section 203 of UMRA, 2 U.S.C. 1533, which supplements section 204(a), provides that before establishing any regulatory requirements that might significantly or uniquely affect small governments, the agency shall have developed a plan that, among other things, provides for notice to potentially affected small governments, if any, and for a meaningful and timely opportunity to provide input in the development of regulatory proposals. The Department is currently preparing a regulatory impact analysis, and the Department will seek input from state and local governments that may be impacted by the regulations under Section 550.

5. National Environmental Policy Act

Congress directed the Secretary to issue these interim final regulations no later than six months after the date of enactment of the Fiscal Year 2007 Homeland Security Appropriations Act. Congress also directed that each chemical facility develop and implement site security plans, with the proviso that the facility could select layered security measures to appropriately address the vulnerability assessment and the risk-based performance standards for security of the facility. Additionally, Congress mandated that the Secretary could not disapprove a site security plan based on the presence or absence of a particular security measure, but only on the failure to satisfy a risk-based performance standard. With that statutory direction in mind, the Department reviewed the rulemaking process with regard to the National Environmental Policy Act (NEPA). First and foremost, the Department is not funding or directing a specific action under these regulations, but issuing performance standards. Chemical facilities are of a wide variety of designs and sizes, and are located in a wide range of geographic settings, communities, and natural environments. Consequently, the Department would have no way to determine the action the chemical facility would take in meeting the standard, and what effect that action might have on the environment. Second, even if the Department could predict the actions the facilities would take in response to the standards, it is likely facilities would take widely varying actions to comply, based upon type of facility, geographic location, existing infrastructure, etc. The Department determined that even if appropriate, it could not reasonably accomplish an Environmental Impact Statement within the six months time allotted for issuance of the interim final regulations.

List of Subjects in 6 CFR Part 27

Chemical security, Facilities, Reporting and recordkeeping, Security measures.

Advance Notice

For the reasons set forth in the preamble, the Department of Homeland Security proposes to add Part 27 to Title 6, Code of Federal Regulations, to read as follows:

PART 27—CHEMICAL FACILITY ANTI-TERRORISM STANDARDS

Subpart A—General

Sec.

Subpart B—Chemical Facility Security Program

Subpart C—Remedies

Subpart D—Other

Authority: Pub. L. 109–295, sec. 550.

Subpart A—General

§ 27.100 Definitions.

Alternative Security Program or *ASP* shall mean a third-party or industry organization program, a local authority, state or Federal government program or any element or aspect thereof, that the Assistant Secretary has determined is sufficient to serve the purposes of this subchapter.

Assistant Secretary shall mean the Assistant Secretary for Infrastructure Protection, Department of Homeland Security, or any other official identified by the Under Secretary as having authority for a specific action or activity under these regulations.

Chemical Facility or *facility* shall mean any facility that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criterion identified by the Department. As used herein, the term chemical facility or facility shall also refer to the owner or operator of the chemical facility. Where multiple owners and/or operators function within a common infrastructure or within a single fenced area, the Assistant Secretary may determine that such owners and/or operators constitute a single chemical facility or multiple chemical facilities depending on the circumstances.

Coordinating Official shall mean the person selected by the Assistant Secretary to ensure that the regulations are implemented in a uniform, impartial, and fair manner.

Covered Facility shall mean a chemical facility determined by the Assistant Secretary to present high levels of security risk, or a facility that the Assistant Secretary has determined is presumptively high risk under § 27.200.

Department shall mean the Department of Homeland Security.

General Counsel shall mean the General Counsel of the Department of Homeland Security or his designee.

Operator shall mean a person who has responsibility for the daily operations of a facility or facilities subject to this part.

Owner of a chemical facility shall mean the person or entity that owns any facility subject to this part.

Present high levels of security risk and *high risk* shall refer to a chemical facility that, in the discretion of the Secretary of Homeland Security, presents a high risk of significant adverse consequences for human life or health, national security and/or critical economic assets if subjected to terrorist attack, compromise, infiltration, or exploitation.

Risk-based tier shall mean a system of ''tiers'' differentiating among covered facilities by risk.

Risk profiles shall mean criteria identified by the Assistant Secretary for determining which chemical facilities will complete the ''Top-screen'' process or provide other risk assessment information.

Secretary, or *Secretary of Homeland Security* shall mean the Secretary of the Department of Homeland Security or any person, officer or entity within the Department to whom the Secretary's authority under Section 550 is delegated.

Terrorist attack or *terrorist incident* shall mean any incident or attempt that constitutes terrorism or terrorist activity under 6 U.S.C. 101(15) or 18 U.S.C. 2331(5) or 8 U.S.C. 1182(a)(3)(B)(iii), including any incident or attempt that involves or would involve sabotage of chemical facilities or theft, misappropriation or misuse of a dangerous quantity of chemicals.

Top-screen process shall mean an initial computerized or other screening process identified by the Assistant Secretary through which chemical facilities provide information to the

Department for use pursuant to § 27.200 of these regulations.

Undersecretary shall mean the Undersecretary for Preparedness or any successors to that position within the Department.

§ 27.105 Applicability.

(a) This part applies to chemical facilities and to covered facilities as set out herein.

(b) This part does not apply facilities regulated pursuant to the Maritime Transportation Security Act of 2002, Pub. L. 107–295, as amended; Public Water Systems, as defined by section 1401 of the Safe Drinking Water Act, Pub. L. 93–523, as amended; Treatment Works as defined in section 212 of the Federal Water Pollution Control Act, Pub. L. 92–500, as amended; any facility owned or operated by the Department of Defense or the Department of Energy, or any facility subject to regulation by the Nuclear Regulatory Commission.

§ 27.110 Implementation.

The Assistant Secretary may implement the Section 550 program in a phased manner, selecting certain chemical facilities for expedited initial processes under these regulations and identifying other chemical facilities or types or classes of chemical facilities for other phases of program implementation. The Assistant Secretary has flexibility to designate particular chemical facilities for specific phases of program implementation based on potential risk or any other factor consistent with these rules.

§ 27.115 Designation of a coordinating official; Consultations and technical assistance.

(a) The Assistant Secretary will have responsibility for ensuring that these regulations are implemented in a uniform, impartial and fair manner, and will designate a Coordinating Official for that purpose.

(b) The Coordinating Official and his staff shall be available to consult at any stage in the processes hereunder with a covered facility regarding compliance with this Part and shall, as necessary and to the extent that resources permit, provide technical assistance to an owner or operator who seeks such assistance.

(c) In order to initiate consultations or seek technical assistance, a covered facility may contact the Coordinating Official.

§ 27.120 Severability.

If a court finds this part, or any portion thereof, to have been promulgated without proper authority, the remainder of this Part will remain in full effect.

Subpart B—Chemical Facility Security Program

§ 27.200 Information regarding security risk for a chemical facility.

(a) In order to determine the security risk posed by chemical facilities, the Secretary may, at any time, request information from chemical facilities that may reflect potential vulnerabilities to a terrorist attack or incident, including questions specifically related to the nature of the business and activities conducted at the facility; the names, nature, conditions of storage, quantities, volumes, properties, major customers, major uses, and other pertinent information about specific chemicals or chemicals meeting a specific criteria; the security, safety, and emergency response practices, operations, procedures; information regarding incidents, history, funding, and other information bearing on the effectiveness of the security, safety and emergency response programs, and other information as necessary. The Assistant Secretary may seek such information by contacting chemical facilities individually or by publishing a notice in the **Federal Register** seeking information from chemical facilities who meet specified risk profiles. The Assistant Secretary may request that such facilities complete a Top-screen process through a secure Department Web site or through other means.

(b) If a chemical facility subject to paragraph (a) of this section fails to provide information requested or complete the Top-screen process within a reasonable period, the Assistant Secretary may, after attempting to consult with the facility, reach a preliminary determination, based on the information then available, that the facility presumptively presents a high level of security risk. The Assistant Secretary shall then issue a notice to the entity of this determination and, if necessary, order the facility to provide information or complete the Top-screen process pursuant to these rules. If the facility then fails to do so, it may be subject to penalties pursuant to § 27.305, audit and inspection under § 27.245 or, if appropriate, an order to cease operations under § 27.310.

(c) If the facility completes the Top-screen process and the Department determines that it does not present a high level of security risk under § 27.205, its status as ''presumptively high risk'' will terminate, and the Department will issue a notice to the facility to that effect.

§ 27.205 Determination that a chemical facility ''Presents A High Level Of Security Risk''.

(a) *Initial Determination.* The Assistant Secretary may determine at any time that a chemical facility presents a high level of security risk based on any information available (including any information submitted to the Department under § 27.205(b) of these regulations) that, in the Secretary's discretion, indicates the potential that a terrorist attack involving the facility could result in significant adverse consequences for human life or health, national security or critical economic assets. Upon determining that a facility presents a high level of security risk, the Department shall notify the facility in writing of such determination and may also notify the facility of the Department's preliminary determination of the facility's placement in a risk-based tier.

(b) *Redetermination.* If a covered facility previously determined to present a high level of security risk has materially altered its operations, it may seek a redetermination by filing a Request for Redetermination with the Assistant Secretary, and may request a meeting regarding the Request. Within 45 calendar days of receipt of such a Request, or within 45 calendar days of a meeting under this paragraph, the Assistant Secretary shall notify the covered facility in writing of the Department's decision on the Request for Redetermination.

(c) *Objection.*

(1) Within 20 calendar days of an Initial Determination or within 20 calendar days of a denial of a Request for Redetermination, the covered facility may file an Objection to an initial determination under paragraph (a) of this section or a redetermination under paragraph (b) of this section with the Assistant Secretary. The Objection should include the name, mailing address, phone number, and email address of the owner/operator of the facility who is filing the Objection and the address of the covered facility which has been deemed to present a high level of security risk. The Objection should indicate the reasons that the covered facility does not present a high level of security risk. The covered facility may request a meeting with the Assistant Secretary, which shall be scheduled within 20 calendar days of the date that the Assistant Secretary receives the Objection. Within 20 calendar days of the filing of an Objection, or if a meeting is requested under this subsection within 20 calendar days of such meeting, the Assistant Secretary shall notify the covered facility in writing of

a final determination whether the facility presents a high level of security risk.

(2) The Assistant Secretary shall issue appropriate guidance and any necessary forms for an Objection or Request for Redetermination covered by this subsection and procedures for notifications made or meetings conducted under this subsection. If additional information from a covered facility is necessary for the Department to address an Objection or Request for Redetermination, the Assistant Secretary may request such information and, in his discretion, toll the running of the timeframes hereunder pending receipt of such information.

(3) Neither an Objection nor a Request for Redetermination shall toll any applicable timeline for a facility to file a Vulnerability Assessment or Site Security Plan, but the Assistant Secretary may extend applicable deadlines pending resolution of an Objection or Request whenever he deems such an extension appropriate.

(4) Failure to file an Objection in accordance with the procedures and time limits contained in this section results in the determination in paragraph (a) of this section or the redetermination in paragraph (b) of this section becoming final agency action.

(5) Any decision made by the Assistant Secretary under paragraph (c)(1) of this section constitutes final agency action for determining whether a chemical facility presents a high level of risk.

§ 27.210 Submissions schedule.

(a) *Vulnerability Assessment and Site Security Plan.* At the time a covered facility is notified of a determination that it is a high risk chemical facility under § 27.205, the Assistant Secretary shall notify the covered facility of its deadlines for completion and submission of a Vulnerability Assessment and Site Security Plan. The presumptive period for filing a Vulnerability Assessment with the Department shall be 60 calendar days from the date of such notification, and 120 calendar days for development and submission of a Site Security Plan. Upon request of the covered facility, the Assistant Secretary may shorten or extend these time periods based on the complexity of the facility, the nature of the covered facility vulnerabilities, the level and immediacy of security risk or for other reasons.

(b) *Alternative Schedules.* For covered facilities under an ASP or for whom the Assistant Secretary accepts, in whole or part, a preexisting assessment of vulnerabilities, or which present other special circumstances, the Assistant Secretary may set an alternative schedule for submissions.

(c) The Assistant Secretary may provide technical assistance to any covered facility in completing the Vulnerability Assessment or Site Security Plan.

§ 27.215 Vulnerability assessments.

(a) *Initial Assessment.* If the Assistant Secretary determines that a chemical facility is high-risk, the facility must complete a Vulnerability Assessment. A Vulnerability Assessment shall include:

(1) Asset Characterization, including identification of potential critical assets; identification of hazards and consequences of concern for the facility and its surroundings and supporting infrastructure, and identification of existing layers of protection;

(2) Threat Assessment, including a description of possible internal threats, external threats, and internally-assisted threats;

(3) Vulnerability Analysis, including the identification of potential vulnerabilities and the identification of existing countermeasures and their level of effectiveness in reducing those vulnerabilities;

(4) Risk Assessment, including a determination of the relative degree of risk to the facility in terms of the expected effect on each critical asset and the likelihood of a successful attack; and

(5) Countermeasures Analysis, including strategies that reduce the probability of a successful attack, strategies that enhance the degree of risk reduction, the reliability and maintainability of the options, the capabilities and effectiveness of mitigation options, and the feasibility of the options.

(b) The Assistant Secretary may require such a covered facility to complete the assessment using an appropriate methodology identified or issued by the Assistant Secretary or through other means and may issue guidance and provide technical assistance regarding such process or methodology. The Assistant Secretary may accept Vulnerability Assessments, in whole or in part, in any sufficient form or format (either pursuant to a general ASP approval or for a particular facility) so long as the vulnerabilities of the covered facility are, in the Assistant Secretary's discretion, sufficiently assessed. The Assistant Secretary may, at his discretion, accept an existing covered facility's Vulnerability Assessment, subject to any necessary revisions or supplements.

(c) *Updates and Revisions.* (1) A covered facility must update, revise or otherwise alter its Vulnerability Assessment to account for new or differing modes of potential terrorist attack or for other security-related reasons, if requested by the Assistant Secretary.

(2) The Assistant Secretary may require that covered facilities periodically review and update risk assessments in accordance with a risk assessment methodology specified or developed by the Department. The Assistant Secretary shall set, and covered facilities shall comply with, a schedule for any such reviews or updates taking into account the dates of the original submissions of Vulnerability Assessments, the risk-based tier(s) of the covered facilities at issue, and other factors bearing on covered facilities' vulnerabilities. These schedules will be mailed either to individual facilities or published as a Notice in the **Federal Register**.

(3) If not otherwise addressed in a schedule for updates, the covered facility must notify the Department of material modifications to the Vulnerability Assessment by submitting a copy of the revised Vulnerability Assessment. If the revision will result in a disapproval of the Vulnerability Assessment, the Department will notify the facility within 30 days of receipt of the revised assessment. It is presumed that material modifications will not result in a disapproval of the Vulnerability Assessment.

§ 27.220 Tiering.

(a) Confirmation or Alteration of Risk-Based Tiering: Following review of a covered facility's Vulnerability Assessment, the Assistant Secretary shall notify the covered facility of its placement within a risk-based tier, or for covered facilities previously notified of a preliminary tiering, confirm or alter such tiering. The Assistant Secretary may provide the facility with guidance regarding the risk-based performance standards and any other necessary guidance materials applicable to its assigned tier.

(b) Objection to Risk-Based Tiering:

(1) A covered facility may contest its placement in a risk-based tier by submitting an Objection to the Assistant Secretary within 20 days of notification under paragraph (a) of this section. The Objection should include the name, mailing address, phone number, and e-mail address of the owner/operator of the covered facility who is filing the Objection and the address of the chemical facility which has been placed in a risk-based tier. The Objection

should indicate the reasons that the covered facility is not in the appropriate risk-based tier. The covered facility may request a meeting with the Assistant Secretary, which shall be scheduled within 20 calendar days of the date that the Assistant Secretary receives the Objection. Within 20 calendar days of the filing of an Objection, or if a meeting is requested under this paragraph within 20 calendar days of such meeting, the Assistant Secretary shall notify the covered facility in writing of a final determination as to the appropriate tier.

(2) The Assistant Secretary may issue appropriate guidance and any necessary forms for such an Objection and procedures for notifications made or meetings conducted under this subsection. If additional information from a covered facility is necessary for the Department to address an Objection, the Assistant Secretary may request such information and toll the running of the timeframes hereunder pending receipt of such information.

(3) An Objection shall not toll any applicable timeline for a covered facility to file a Vulnerability Assessment or Site Security Plan, but the Assistant Secretary may extend applicable deadlines pending resolution of the Objection whenever he deems such an extension appropriate.

(4) Failure to file an Objection in accordance with the procedures and time limits contained in this section results in the determination in paragraph (a) of this section becoming final agency action.

(5) Any decision made by the Assistant Secretary under paragraph (b)(1) of this section constitutes final agency action for tiering.

§ 27.225 Site security plans.

(a) Covered facilities shall submit a Site Security Plan as directed by the Assistant Secretary. The Site Security Plan must meet the following standards:

(1) Address each vulnerability identified in the facility's Vulnerability Assessment and identify and describe the security measures to address each such vulnerability;

(2) Identify and describe how security measures selected by the facility will address the applicable risk-based performance standards and potential modes of terrorist attack including, as applicable, vehicle-borne explosive devices, water borne explosive devices, ground assault, or other modes of potential modes identified by the Department;

(3) Identify and describe how security measures selected and utilized by the facility will address each applicable performance standard for the appropriate risk-based tier for the facility; and

(4) Specify other information the Assistant Secretary deems necessary regarding chemical facility security.

(b) *Updates and Revisions.*

(1) When a covered facility updates, revises or otherwise alters its Vulnerability Assessment pursuant to § 27.215(b), the covered facility shall make corresponding changes to its Site Security Plan.

(2) The Assistant Secretary may also require that covered facilities periodically review and update Site Security Plans taking into account the dates of the original submission of the Site Security Plan, the risk-based tier(s) of the covered facility at issue, and other factors as determined by the Assistant Secretary. The Assistant Secretary shall set, and covered facilities shall comply with, a schedule for any such reviews or updates. These schedules will be mailed either to individual facilities or published as a Notice in the **Federal Register**.

(3) If not otherwise addressed in a schedule for updates, the covered facility must notify the Department of material modifications to the Site Security Plan by submitting a copy of the revised Site Security Plan. If the revision will result in a disapproval of the Site Security Plan, the Department will notify the facility within 30 days of receipt of the revised plan. It is presumed that material modifications will not result in a disapproval of the Site Security Plan.

§ 27.230 Risk-based performance standards.

(a) Covered facilities must satisfy the performance standards identified in this section. The Assistant Secretary will issue guidance on the application of these standards to risk-based tiers of covered facilities. Each covered facility must select, develop, and implement measures designed to:

(1) Secure and monitor the perimeter of the facility;

(2) Secure and monitor restricted areas or potentially critical targets within the facility;

(3) Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including,

(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and

(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures;

(4) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;

(5) Secure and monitor the shipping and receipt of hazardous materials for the facility;

(6) Deter theft or diversion of potentially dangerous chemicals;

(7) Deter insider sabotage;

(8) Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, Supervisory Control And Data Acquisition (SCADA) systems, and other sensitive computerized systems;

(9) Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;

(10) Maintain effective monitoring, communications and warning systems, including

(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;

(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and

(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

(11) Ensure proper security training, exercises, and drills of facility personnel;

(12) Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or potentially critical targets;

(13) Escalate the level of protective measures for periods of elevated threat;

(14) Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;

(15) Report significant security incidents to the Department;

(16) Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;

(17) Establish official(s) and an organization responsible for security and for compliance with these standards;

(18) Maintain appropriate records; and

(19) Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;

(20) Address any additional performance standards the Assistant Secretary may specify.

§ 27.235 Alternative security program.

The Assistant Secretary may approve in whole, in part, or subject to revisions or supplements, an Alternative Security Program (ASP) for covered facilities required to have Vulnerability Assessments and Site Security Plans under this part upon a determination by the Assistant Secretary that the Alternative Security Program meets the requirements of this part.

§ 27.240 Review and approval of vulnerability assessments and site security plans.

(a) *Review and Approval.*

(1) Covered facilities must provide Vulnerability Assessments and Site Security Plans to the Department:

(i) Within the time period that the Department specifies in schedule that it provides to the facility, or

(ii) If no schedule is provided to a particular facility, within the time period specified by Notice in the **Federal Register**.

(2) The Department will review and approve or disapprove all Vulnerability Assessments and Site Security Plans, including Alternative Security Plans pursuant to § 27.235, submitted to the Department.

(i) Vulnerability Assessments. The Department will approve all Vulnerability Assessments that satisfy the requirements of § 27.215.

(ii) Site Security Plans. The Department will review Site Security Plans through a two-step process. Upon receipt of Site Security Plan from the covered facility, the Department will review the documentation and make a preliminary determination as to whether it satisfies the requirements of § 27.225. If the Department finds that the requirements are satisfied, the Department will issue a Letter of Authorization to the covered facility. Following issuance of the Letter of Authorization, the Department will inspect the covered facility in accordance with § 27.245 for purposes of determining compliance with the requirements of this part.

(3) The Department will not disapprove a Site Security Plan submitted under this Part based on the presence or absence of a particular security measure. The Department may disapprove a Site Security Plan that fails to satisfy the risk-based performance standards established in § 27.230.

(b) When the Department disapproves a Vulnerability Assessment, a preliminary Site Security Plan issued prior to inspection, or a Site Security Plan following inspection, the Department will provide the facility with a written notification that includes a clear explanation of deficiencies in the Vulnerability Assessment or Site Security Plan. The facility shall then enter further consultations with the Department and resubmit a sufficient Vulnerability Assessment or Site Security Plan by the time specified in the written notification provided by the Department under this section. Alternatively, the facility may file an objection under paragraph (c) of this section.

(c) *Objection to Disapproval of Site Security Plan.*

(1) A covered facility may contest the disapproval of its Site Security Plan by submitting an Objection to Assistant Secretary within 20 days of notification under paragraph (b) of this section. The Objection should include the name, mailing address, phone number, and email address of the owner/operator of the facility who is filing the Objection and the address of the chemical facility which has had its Site Security Plan disapproved. The Objection should indicate the reasons why the facility's Site Security Plan should be approved. The covered facility may request a meeting with the Assistant Secretary, which shall be scheduled within 20 calendar days of the date that the Assistant Secretary receives the Objection. Within 20 calendar days of the filing of an Objection, or if a meeting is requested under this subsection within 20 calendar days of such meeting, the Assistant Secretary shall notify the covered facility in writing of a final determination as to approval of its Site Security Plan.

(2) The Assistant Secretary may issue appropriate guidance and any necessary forms for such an Objection and procedures for notifications made or meetings conducted under this subsection. If additional information from a covered facility is necessary for the Department to address an Objection, the Assistant Secretary may request such information and toll the running of the timeframes hereunder pending receipt of such information.

(3) A covered facility may contest a final determination made under paragraph (c)(1) of this section by filing an appeal pursuant to § 27.320.

§ 27.245 Inspections and audits.

(a) Authority. In order to assess compliance with the requirements of this part, authorized DHS officials may enter, inspect, and audit the property, equipment, operations, and records of covered facilities. Except for the higher-risk tiers of covered facilities, the Department may certify third-party auditors to perform audits and inspections.

(b) Following preliminary approval of a Site Security Plan in accordance with § 27.225, the Department or a certified third-party auditor will inspect the covered facility for purposes of determining compliance with the requirements of this part.

(1) If after the inspection, the Department determines that the requirements of § 27.225 have been met, the Department will issue a Letter of Approval to the covered facility.

(2) If after the inspection, the Department determines that the requirements of § 27.225 have not been met, the Department will proceed as directed by § 27.240(b).

(c) Time and Manner. Authorized DHS officials will conduct audits and inspections at reasonable times and in a reasonable manner. DHS will provide covered facility owners and/or operators with 24-hour advance notice before inspections, except where the Under Secretary or Assistant Secretary determines that an inspection without such notice is warranted by exigent circumstances and approves such inspection.

(d) The Assistant Secretary shall issue guidance identifying appropriate processes for such inspections, and specifying the type and nature of documentation that must be available on site.

§ 27.250 Recordkeeping requirements.

(a) Except as provided in § 27.250(b), the covered facility must keep records of the activities as set out below for at least 3 years and make them available to DHS upon request. The following records must be kept:

(1) Training. For training, the date and location of each session, time of day and duration of session, a description of the training, the name and qualifications of the instructor, and a clear, legible list of attendees to include the attendee signature;

(2) Drills and exercises. For each drill or exercise, the date held, a description of the drill or exercise, a list of participants, a list of equipment (other than personal equipment) tested or employed in the exercise, the name(s) and qualifications of the exercise director, and any best practices or

lessons learned which may improve the Site Security Plan;

(3) Incidents and breaches of security. Date and time of occurrence, location within the facility, a description of the incident or breach, the identity of the individual to whom it was reported, and a description of the response;

(4) Maintenance, calibration, and testing of security equipment. For each occurrence of maintenance, calibration, and testing, record the date and time, name and qualifications of the technician(s) doing the work, and the specific security equipment involved;

(5) Security threats. Date and time of occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response;

(6) For each audit of the Site Security Plan or a Vulnerability Assessment, a letter certified by the covered facility stating the date the audit was conducted.

(7) All Letters of Authorization and Approval from the Department, and documentation identifying the results of audits and inspections hereunder.

(b) Vulnerability Assessments, Site Security Plans, and all related correspondence with the Department must be retained for at least 6 years.

(c) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized access, deletion, destruction, amendment, and disclosure.

Subpart C—Remedies

§ 27.300 Order for compliance.

(a) Where the Department determines that a chemical facility is in violation of any of the requirements of this part, the Department may issue an Order for Compliance, directing the chemical facility to remedy any instances of noncompliance.

(b) The Order for Compliance shall be signed by the Assistant Secretary, shall be dated, and shall include, at a minimum:

(1) The address of the chemical facility in question;

(2) A listing of the provision(s) that the chemical facility is alleged to have violated;

(3) A statement of facts upon which the alleged violation(s) are based;

(4) A statement, indicating what actions the chemical facility must take to bring its operations into compliance;

(5) The date by which the chemical facility must bring its operations into compliance,

(6) A statement of the chemical facility's right to present written explanations, information, or any materials in answer to the alleged violation(s).

(c) By the compliance date specified in the Order, a representative of the chemical facility shall submit a written response to the Department, explaining how the facility has remedied any instances of noncompliance. A chemical facility may request a consultation meeting with the Assistant Secretary.

§ 27.305 Order assessing civil penalty.

(a) A chemical facility that violates an order issued under § 27.305 is liable to the United States for a civil penalty of not more than $25,000 for each day during which the violation continues.

(b) Where the Department has issued an Order for Compliance under § 27.305, and the chemical facility fails to bring its operations into compliance by the date specified in the Order, the Department may issue an Order Assessing Civil Penalty.

(c) The Order Assessing Civil Penalty shall be signed by the Assistant Secretary, shall be dated, and shall include:

(1) The address of the chemical facility in question;

(2) A listing of the provisions that the chemical facility has violated;

(3) A statement of facts upon which the violation(s) are based;

(4) The amount of civil penalties being assessed against the chemical facility; and

(5) A statement, indicating what actions the chemical facility must take to bring its operations into compliance.

(d) Within 30 calendar days of the date of the Order Assessing Civil Penalty, the chemical facility shall pay the penalty in full or file an Appeal as provided under § 27.320.

§ 27.310 Order to cease operations.

(a) *Generally.* Where the Department has issued an Order for Compliance under § 27.305, and the chemical facility fails to bring its operations into compliance by the date specified in the Order, the Department may initiate proceedings to cease operations at a chemical facility.

(b) *Notice of Intent to Order the Cessation of Operations.* If DHS determines that a chemical facility is not in compliance with the requirements of this part, the Assistant Secretary may issue a Notice of Intent to Order the Cessation of Operations. The Notice shall be signed by the Assistant Secretary, shall be dated, and shall include:

(1) The address of the chemical facility in question;

(2) A clear explanation of the deficiencies in the chemical facility's chemical security program, including, if applicable, any deficiencies in the chemical facility's Vulnerability Assessment and/or Site Security Plan; and

(3) The date, as determined to be appropriate by the Under Secretary under the circumstances, by which the chemical facility must be brought into compliance.

(c) *Response to Notice of Intent to Order the Cessation of Operations.* By the compliance deadline specified in the Notice of Intent to Order the Cessation of Operations, the chemical facility must submit to the Assistant Secretary a written response, which shall include evidence showing that the chemical facility has brought its operations into compliance and an explanation of how the chemical facility has satisfied the deficiencies in its Vulnerability Assessment and Site Security Plan. The chemical facility may request a consultation meeting with the Assistant Secretary.

(d) *Order to Cease Operations.* Where a chemical facility fails to bring its operations into compliance by the date specified in the Notice of Intent to Cease Operations, the Assistant Secretary may issue an Order to Cease Operations. The Order shall be signed by the Assistant Secretary, shall be dated, shall provide a clear explanation of the deficiencies in the chemical facility's chemical security plan, and shall identify a date on which operations must cease. In the absence of an appeal under § 27.320, the Order to Cease Operations will remain in effect until the chemical facility brings its operations into compliance.

§ 27.315 Orders generally.

(a) An Order issued under this subpart shall not constitute final agency action until a chemical facility exhausts all appeals under this subpart or the time for such appeals has lapsed.

(b) An Order issued under this subpart shall be stayed while an appeal under § 27.320 is pending.

(c) The Department may issue appropriate guidance and any necessary forms for the issuance of Orders under this subpart.

§ 27.320 Appeals.

(a) A chemical facility may appeal:

(1) A final determination under § 27.240(c)(1) by submitting an appeal to the Under Secretary;

(2) The decision of the Assistant Secretary to issue an Order For Compliance under § 27.305 or an Order Assessing Civil Penalty under § 27.310 by submitting an appeal to the Under Secretary; and

(3) The decision of the Assistant Secretary to issue an Order to Cease Operations under § 27.315 by submitting an appeal to the Deputy Secretary.

(b) The chemical facility shall file an appeal with the adjudicating official within 30 calendar days of the date the Department makes its final determination or issues an Order. The appeal shall include, at a minimum: the name, mailing address, and contact information of the owner/operator of the chemical facility that is filing the appeal; the address of the chemical facility for which the Department disapproved a Site Security Plan or to which the Department issued an Order; and the reasons why the chemical facility believes the Assistant Secretary's determination made pursuant to § 27.240(c) or order issued pursuant to §§ 27.300, 27.305, or 27.310 should be set aside.

(c) The covered facility may request a consultation meeting with the adjudicating official(s). If requested, the meeting will be scheduled within 30 calendar days of the date that the Department receives the request.

(d) Within 30 calendar days of the filing of an appeal, or if a meeting is requested under this subsection, within 30 days of such a meeting, the adjudicating official shall notify the chemical facility in writing of his decision.

(1) For determinations made pursuant to § 27.240(c), the Under Secretary and General Counsel will be the adjudicating officials and will make a finding that the determination should either be sustained or set aside.

(2) For orders issued pursuant to §§ 27.300 and 27.305, the Under Secretary and General Counsel will be the adjudicating officials, and for orders issued under § 27.310, the Deputy Secretary will be the adjudicating official. The adjudicating official(s) may affirm the order, revoke the order, or suspend the order for a specified period of time, after which the terms of the Order go into effect.

(e) In reviewing the Assistant Secretary's decision to issue an Order under § 27.305, the adjudicating official(s) may, in his discretion, mitigate the civil penalty amount based on the following circumstances: the nature and circumstances of the violation(s); the extent and gravity of the situation; the degree of the facility's culpability; respondent's prior history of offenses; the effect of the penalty on respondent's ability to continue in business; and such other matters as justice may require.

(f) Any decision made by an adjudicating official under paragraph (c) of this section constitutes final agency action.

(g) Failure to file an appeal in accordance with the procedures and time limits contained in this section results in the Assistant Secretary's determination or issuance of an Order becoming final agency action.

(h) The Department may issue appropriate guidance and any necessary forms for appeals and procedures for notifications made or meetings conducted under this paragraph and may, notwithstanding the provisions of this subsection, provide for an immediate or an expedited review appeal with accelerated timeframes for appropriate cause.

(i) If additional information from a covered facility is necessary for the Department to address an appeal, the Under Secretary may request such information and toll the running of the timeframes hereunder pending receipt of such information.

Subpart D—Other

§ 27.400 Chemical-terrorism vulnerability information.

(a) *Applicability.* This section governs the maintenance, safeguarding, and disclosure of information and records that constitute Chemical-terrorism Security and Vulnerability Information (CVI), as defined in paragraph (b) of this section. The Secretary shall administer this Section consistent with section 550, including appropriate sharing with State and local officials, law enforcement officials, and first responders.

(b) *Chemical-terrorism Vulnerability Information.* In accordance with section 550(c) of the Homeland Security Appropriations Act of 2007, the following information shall constitute CVI:

(1) Vulnerability assessments under § 27.215;

(2) Site security plans under § 27.225;

(3) Any documents developed pursuant to § 27.240, relating to the Department's review and approval of vulnerability assessments and security plans;

(4) Alternate security plans under § 27.235;

(5) Documents relating to inspection or audits under § 27.245;

(6) Any records required to be created or retained under § 27.250;

(7) Sensitive portions of orders, notices or letters under §§ 27.300, 27.305, 27.310, and 27.315; and

(8) Information developed pursuant to §§ 27.200 and 27.205.

(9) Any other information that the Secretary, in his discretion, determines warrants the protections set forth in this part.

(c) *Covered Persons.* Persons subject to the requirements of this section are:

(1) Each person who has access to CVI, as specified in section 5 of this part;

(2) Each person receiving CVI in the course of proceedings or litigation under paragraphs (g), (h), and (i) of this section; and

(3) Each person who otherwise receives or gains access to what they know or should reasonably know constitutes CVI.

(d) *Duty to protect information.* A covered person must—

(1) Take reasonable steps to safeguard CVI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of CVI, the person must store it a secure container, such as a safe;

(2) Disclose, or otherwise provide access to, CVI only to covered persons who have a need to know, unless otherwise authorized in writing by the Secretary of DHS;

(3) Refer requests by other persons for CVI to DHS;

(4) Mark CVI as specified in paragraph (f) of this section;

(5) Dispose of CVI as specified in paragraph (k) of this section;

(6) If a covered person receives a record containing CVI that is not marked as specified in paragraph (f) of this section, the covered person must—

(i) Mark the record as specified in paragraph (f) of this section; and

(ii) Inform the sender of the record that the record must be marked as specified in paragraph (f) of this section.

(7) When a covered person becomes aware that CVI has been released to unauthorized persons, the covered person must promptly inform DHS.

(8) In the case of information that is both CVI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act, any covered person who is a Federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under section 214 and any implementing regulations.

(e) *Need to know—In general.*

(1) A person has a need to know CVI in each of the following circumstances:

(i) When the person requires access to specific CVI to carry out chemical facility security activities approved, accepted, funded, recommended, or directed by DHS.

(ii) When the person is in training to carry out chemical facility security activities approved, accepted, funded, recommended, or directed by DHS.

(iii) When the information is necessary for the person to supervise or otherwise manage individuals carrying out chemical facility security activities approved, accepted, funded, recommended, or directed by the DHS.

(iv) When the person needs the information to provide technical or legal advice to a covered person regarding chemical facility security requirements of Federal law.

(v) When the person needs the information to represent a covered person in connection with any judicial or administrative enforcement proceeding regarding those requirements;

(vi) When DHS determines that access is required under sections 27.400(h) or 27.400(i) in the course of a judicial or administrative enforcement proceeding.

(2) *Federal employees, contractors, and grantees.*

(i) A Federal employee has a need to know CVI if access to the information is necessary for performance of the employee's official duties.

(ii) A person acting in the performance of a contract with or grant from DHS has a need to know CVI if access to the information is necessary to performance of the contract or grant.

(3) *Background check.* DHS may make an individual's access to the CVI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding CVI that are satisfactory to DHS.

(i) *Need to know further limited by the DHS.* For some specific CVI, DHS may make a finding that only specific persons or classes of persons have a need to know.

(ii) [Reserved].

(f) *Marking of paper records.*

(1) In the case of paper records containing CVI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of—

(i) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(ii) Any title page; and

(iii) Each page of the document.

(2) Protective marking. The protective marking is: CHEMICAL–TERRORISM VULNERABILITY INFORMATION.

(3) Distribution limitation statement. The distribution limitation statement is:

WARNING: This record contains Chemical-terrorism Vulnerability Information that is controlled under 6 CFR 27.400. No part of this record may be disclosed to persons without a ''need to know,'' as defined in 6 CFR 27.400(e), except with the written permission of the Secretary of Homeland Security. Unauthorized release may result in civil penalty or other action. For DHS, public disclosure is governed by 6 CFR 27.400(g).

(4) Other types of records. In the case of non-paper records that contain CVI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

(g) *Disclosure by DHS—In general.*

(1) Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing CVI are not available for public inspection or copying, nor does DHS release such records to persons without a need to know.

(2) *Disclosure under the Freedom of Information Act and the Privacy Act.* If a record contains both CVI and information that is not CVI, DHS, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the CVI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(h) *Disclosure in administrative enforcement proceedings.*

(1) DHS may provide CVI to a person governed by section 550 in the context of an administrative enforcement proceeding when, in the sole discretion of DHS, as appropriate, access to the CVI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by DHS.

(2) *Security background check.* Prior to providing CVI to a person under section 27.400(h)(1), DHS may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of DHS, a security background check.

(i) *Disclosure in civil or criminal litigation.*

(1) In any judicial enforcement proceeding, whether civil or criminal, the Secretary, in his sole discretion, may, subject to section 27.400(i)(1)(A), authorize access to CVI for persons necessary for the conduct of such proceedings, provided that no other persons not so authorized shall have access to or be present for the disclosure of such information.

(i) Security background check. Prior to providing CVI to a person under paragraph (a) of this section, DHS may require the individual to undergo and satisfy, in the judgment of DHS, a security background check.

(ii) [Reserved].

(2) In any judicial enforcement proceeding, whether civil or criminal, where a person seeks to disclose CVI to a person not authorized to receive it under this part, or where a person not authorized to receive CVI under this part seeks to compel its disclosure through discovery, the United States may make an ex parte application in writing to the court seeking authorization to—

(i) Redact specified items of CVI from documents to be introduced into evidence or made available to the defendant through discovery under the Federal Rules of Civil Procedure;

(ii) Substitute a summary of the information for such CVI; or

(iii) Substitute a statement admitting relevant facts that the CVI would tend to prove.

(3) The court shall grant a request under paragraph (i)(2) of this section if, after in camera review, the court finds that the redacted item, stipulation, or summary is sufficient to allow the defendant to prepare a defense.

(4) If the court enters an order granting a request under paragraph (i)(2) of this section, the entire text of the documents to which the request relates shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

(5) If the court enters an order denying a request of the United States under paragraph (b) of this section, the United States may take an immediate, interlocutory appeal of the court's order in accordance with 18 U.S.C. 2339B(f)(4), (5). For purposes of such an appeal, the entire text of the documents to which the request relates, together with any transcripts of arguments made ex parte to the court in connection therewith, shall be maintained under seal and delivered to the appellate court.

(6) Except as provided otherwise at the sole discretion of the Secretary, access to CVI shall not be available in any civil litigation unrelated to the enforcement of section 550.

(7) Taking of trial testimony—

(i) *Objection*—During the examination of a witness in any judicial proceeding, the United States may object to any question or line of inquiry that may

require the witness to disclose CVI not previously found to be admissible.

(ii) *Action by court*—In determining whether a response is admissible, the court shall take precautions to guard against the compromise of any CVI, including—

(A) Permitting the United States to provide the court, ex parte, with a proffer of the witness's response to the question or line of inquiry; and

(B) Requiring the defendant to provide the court with a proffer of the nature of the information that the defendant seeks to elicit.

(iii) *Obligation of defendant*—In any judicial proceeding, it shall be the defendant's obligation to establish the relevance and materiality of any CVI sought to be introduced.

(8) Construction. Nothing in this subsection shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information, including the invocation of the military and State secrets privilege.

(j) *Consequences of Violation.* Violation of this section is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of CVI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

(k) *Destruction of CVI.*

(1) DHS. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DHS destroys CVI when no longer needed to carry out the agency's function.

(2) Other covered persons.

(A) *In general.* A covered person must destroy CVI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the CVI to carry out security measures.

(B) *Exception.* Section 27.400(k)(2) does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

§ 27.405 Review and preemption of State laws and regulations.

(a) No law, regulation, or administrative action of a State or political subdivision thereof, nor any decision or order rendered by a court under state law, shall have any effect if such law, regulation, or decision conflicts with, hinders, poses an obstacle to or frustrates the purposes of these regulations or of any approval, disapproval or order issued thereunder.

(b) State law, regulation or administrative action defined.—For purposes of this section, the phrase ''State law, regulation or administrative action'' means any enacted law, promulgated regulation, ordinance, administrative action, order or decision, or common law standard of a State or any of its political subdivisions.

(c) Submission for review.—Any chemical facility covered by these regulations and any State may petition the Department by submitting a copy of a State law, regulation, or administrative action, or decision or order of a court for decision under this section.

(d) Review and decision.

(1) Review. The Department will review State laws, administrative actions, or decisions or orders of a court under State law and regulations submitted under this section, and will opine whether—

(i) Complying with the State law or regulation and a requirement of this Part is not possible; or

(ii) The application or enforcement of the State law or regulation would present an obstacle to or frustrate the purposes of this Part.

(2) Decision. The Department may issue a written opinion on any question regarding preemption. If the Department determines that a State law or regulation should not be preempted, he may issue a written decision explaining the decision. The Assistant Secretary will notify the petitioner and the Attorney General of the subject State (if such State has not petitioned the Department under this section) of any decision under this section.

§ 27.410 Third party actions.

(a) Nothing in this Part shall confer upon any person except the Secretary a right of action, in law or equity, for any remedy including, but not limited to, injunctions or damages to enforce any provision of this section.

(b) An owner or operator of a chemical facility may petition the Assistant Secretary to provide the Department's view in any litigation involving any issues or matters regarding this Part.

Dated: December 21, 2006.

Michael Chertoff,

Secretary of Homeland Security, Department of Homeland Security.

Note: The following appendices will not appear in the Code of Federal Regulations.

Appendix A

The Department believes that ''risk'' in the context of terrorism is a function of three variables: consequence (or criticality), vulnerability (or the likelihood that an attack will succeed if launched), and threat (or the likelihood that an attack would be launched in the first place). The Department also believes that ''consequence'' is the initial qualifying factor—that is, if a thing is not critical, then there will not be a significant level of risk associated with it. Accordingly, the Department intends to employ a consequence-only ''Top-screen.''

I. Purpose of the Top-Screen Tool

The Top-screen is a basic questionnaire that facilities will be required to complete. It will provide the Department with information to make a preliminary determination as to the level of risk associated with any given facility. The Department will use it to screen facilities in order to eliminate as many as is appropriate from further activity under the regulation, and to prioritize those facilities that are, on preliminary assessment, ''high risk.'' The Department will make the Top-screen available as an on-line tool.

II. Categories of Top-Screen Users

There will be two categories of Top-screen users: providers and submitters. A provider is a qualified individual familiar with the facility in question. This person will complete the screening tool. A submitter is an officer of the corporation (or equivalent) responsible for the facility in question. The submitter will send the completed Top-screen(s) to DHS, and in so doing, will attest to the accuracy of the information provided.

The provider and the submitter may be the same person should a facility owner/operator so choose. The provider will therefore have the option of ''submitting'' the completed Top-screen to DHS or forwarding it to the provider within his or her own organization.

DHS is considering the imposition of a requirement whereby the submitter must satisfy all of the following requirements: be an officer of the corporation, be a citizen of the United States, and be domiciled in the United States. The Department requests comment on this proposed requirement.

III. Top-Screen Questions

The first segment of the Top-screen will focus on gathering identifying information from the facility, such as its name, address, identification numbers, corporate affiliation, and geo-location. During this segment, DHS will obtain essential contact information and will learn of the exact location of facilities.

The first segment of the Top-screen will also seek to gather information on criticality issues. It will ask questions directed at identifying criticality related to the:

- Potential loss of life (and life-changing injuries) on or near the facility;
- Potential loss of the capability to execute a critical mission, not only in defense, but also in governance and in the provision of essential services and utilities.

The second segment of the Top-screen will ask a series of exclusionary questions. For example, DHS will ask whether a facility is

a public water system or a water treatment works facility, covered under MTSA, owned or operated by the Department of Defense or the Department of Energy, and/or licensed by the Nuclear Regulatory Commission. By asking these questions, DHS will be able to quickly ''screen out'' those facilities that are excluded by law from this regulation, yet will still be able to account for those facilities and to know why they are excluded from the regulation.

To address risk to human life, the third segment of the Top-screen will focus on identifying which chemicals are present at facilities. As part of the Top-screen tool, DHS will provide a list of chemicals and threshold quantities (TQ) for each listed chemical. A provider would be able to select (possibly through the use of a pull-down menu) those chemicals that are present (at any time or in the course of a year, depending on the chemical) in quantities equal to or above the stated TQ. Where the facility does not contain any such chemicals, the facility will be presumptively screened out of coverage from the regulation.

This segment will be broken down into several ''pages,'' each of which addresses the security issues associated with specific chemicals and the TQs of those chemicals. In most (but not all) cases, these security issues will parallel the Department of Transportation's classes of hazards.

To address human health and safety consequences, the tool would ask the facility the following types of questions:

- Whether a toxic release worst-case scenario (as identified by the facility under the EPA Risk Management Program) might expose a residential population greater than or equal to 200,000 persons, and if so, whether the distance in such a scenario might exceed 25 miles;
- Whether a flammable release worst-case scenario (as identified by the facility under the EPA Risk Management Program) might expose a residential population greater than or equal to 1,000 persons;
- Whether the facility manufactures or stores explosive materials in sufficient quantities to result in an offsite residential exposed population;
- Whether the facility has any specified chemical weapon or chemical weapon precursors; To address economic impacts, the tool would ask the facility the following types of questions:
- Whether the facility produces products of national economic importance or whose loss could negatively impact multiple economic sectors;
- Whether an attack on the facility could cause collateral physical damage to key transportation assets;

To address mission impacts the tool would ask questions, such as whether the facility:

- Has chemical(s) for which it provides 35% of the U.S. domestic production capacity;
- Is the sole U.S. supplier;
- Produces a chemical or product used in the manufacture of defense weapons;
- Produces a chemical or product supplied to and for use by multiple defense weapons systems contractors;
- Is a major chemical supplier (>35% market share) to DoD for reasons other than defense weapons systems;
- Produces a chemical or product directly to another manufacturer, producer, or distributor for subsequent use in the manufacture of defense weapons systems;
- Serves as a major or sole supplier to a public health, water treatment, or power generation facility;

The Top-screen tool has the ability to calculate populations at risk and other potential consequences based upon factors such as geo-location and type and quantity of chemical without further information from the provider. The Top-screen tool will be part of a sophisticated system that allows the importation of data from the National Geospatial-Intelligence Agency (NGA) and other such data repositories, as well as the importation and use of modeling tools from the National Laboratories System. Accordingly, DHS will calculate consequentiality based upon the data that facilities provide during the Top-screen process.

Appendix B

Background: Risk Analysis and Management for Critical Asset Protection (RAMCAP) Vulnerability Assessment Methodology

Preface

RAMCAP is an overall strategy and methodology to allow for a more consistent and systematic analysis of the terrorist threat and vulnerabilities against the U.S. infrastructure using a risk-based framework. RAMCAP was developed under contract to DHS by the American Society of Mechanical Engineers Innovative Technologies Institute, LLC (ASME).

As indicated, the Department is considering options for a vulnerability assessment tool for its chemical sector security program and invites comments on available options, including the elements of the process described below.

The Department thanks the Center for Chemical Process Safety (CCPS), the American Petroleum Institute (API), and the National Petrochemical & Refiners Association (NPRA) all of whom agreed to make their VA Methodology and other materials available to DHS as a reference to support the effort to produce a methodology that would support the Department's needs.

RAMCAP Vulnerability Assessment Methodology

General

The Risk Analysis and Management for Critical Asset Protection (RAMCAP) approach to risk analysis was developed for the Department to be broadly applicable to all critical infrastructure sectors. RAMCAP can assist with an overall strategy and methodology to allow for a more consistent and systematic analysis of the terrorist threat and vulnerabilities against the U.S. infrastructure using a risk-based framework. Phase 1 of the project developed the overall risk framework while Phase 2 was the further refinement and development of the methodologies at the sector level.

A Sector module includes 2 components—a screening process referred to as a Top-screen, and a vulnerability assessment tool, referred to as the VA.

1. The screening process provides a basis for understanding the critical infrastructures of greatest concern and the magnitude and nature of their significance. The DHS Top-screen to be employed in the implementation of regulations is described in general terms in Appendix A.

2. Vulnerability assessments will provide further vulnerability and consequence information based on several postulated threats of concern.

The threat scenarios to be used for RAMCAP were provided by DHS. The concept is as follows:

1. Each infrastructure would use the same threat scenarios

2. The user would begin by analyzing each of the scenarios on the list. If the facility cannot tolerate or neutralize this threat, or if a higher level of force causes a greater outcome, then the scenario would consider that greater force and analyze it.

3. The facility is not necessarily expected to be able to prevent or protect against the scenario.

This concept provides DHS with the information they require to make decisions about maximum expected consequences for each scenario. In this context, ''threats'' should be viewed as a yardstick employed to ascertain a consistent expression of vulnerability. These ''threats'' should not be seen as either indicative of government knowledge of enemy intent, nor as an expected design basis for security programs.

The RAMCAP methodology produces a relativistic expression of risk.

Objectives

The RAMCAP project creates a set of sector-specific vulnerability assessment tools that are:

- Consistent across sectors
- Appropriate to sector capabilities
- Reflective of asset owner/operator concerns, strengths and weaknesses
- Able to capture those datum points which support DHS information needs

The sector-specific vulnerability assessment tool being developed is:

- Based upon specific metrics, the use of which is repeatable sector to sector; thereby allowing cross-sector comparative risk assessment.
- Designed to employ specific, defined consequence generators (threat scenarios);
- Designed to evaluate:
  - Consequences (impact produced by the defined consequence generator);
  - Vulnerabilities (potential point targets and/or attack vectors, a broadly accepted surrogate for frequency/probability of success of an attack);
  - Countermeasures (including factors in mitigation, deterrent factors, detection factors, delay factors, response capability, and inherent robustness);
  - Actions/countermeasures at different threat levels;
  - Residual security vulnerability (gap analysis).

The purpose for a sector-specific assessment tool is to advance sector organization efforts to:

- Integrate key features of RAMCAP that cover Vulnerability Assessment (including threat and consequence analysis) into existing sector-specific methods, metrics and documentation, or;
- Assist sector organizations in developing new sector-specific Vulnerability Assessment methods, metrics and documentation as appropriate.

Overview of the RAMCAP VA Methodology

The RAMCAP VA process is a risk-based and performance-based methodology. The user can choose different means of accomplishing the general VA method so long as the end result meets the same performance criteria. The overall 5-step approach of the RAMCAP VA methodology is as follows:

Step 1: Asset Characterization

The asset characterization includes analyzing information that describes the technical details of facility assets as required to support the analysis, identifying the potential critical assets, identifying the hazards and consequences of concern for the facility and its surroundings and supporting infrastructure, and identifying existing layers of protection.

Step 2: Threat Assessment

This step involves choosing appropriate threats for the SVA based on a DHS provided sector-level Threat Assessment of the potential threats to the critical infrastructure/key resource (CI/KR) sectors, as well as analysis of how those threats relate to sector vulnerabilities and consequences.

Step 3: Vulnerability Analysis

The vulnerability analysis includes the relative pairing of each target asset and threat to identify potential vulnerabilities related to process security events. This involves the identification of existing countermeasures and their level of effectiveness in reducing those vulnerabilities.

The degree of vulnerability of each valued asset and threat pairing is evaluated by the formulation of security-related scenarios or by an asset protection basis. If certain criteria are met, such as a higher consequence ranking value, then it may be useful to apply a scenario-based approach to conduct the Vulnerability Analysis. It includes the assignment of risk rankings to the security-related scenarios developed. If the asset-based approach is used, the determination of the asset's consequences may be enough to assign a target ranking value and protect via a standard protection set for that target level. In this case, scenarios may not be developed further than the general thought that an adversary is interested in damaging or stealing an asset.

Step 4: Risk Assessment

The risk assessment determines the relative degree of risk to the facility in terms of the expected effect on each critical asset as a function of consequence and probability of occurrence. Using the assets identified during Step 1 (Asset Characterization), the risks are prioritized based on the likelihood of a successful attack. Likelihood is determined by the team after considering the degree of threats assessed under Step 2, and the degree of vulnerability identified under Step 3.

Step 5: Countermeasures Analysis

Since RAMCAP is designed for use in a voluntary program wherein asset owners are only providing certain information to DHS, the asset owner is not required under RAMCAP to make security enhancements. However, within the DHS regulatory structure, the VA will lead directly to the production of a Site Security Plan, which must effectively address the vulnerabilities and risks identified in the VA. Accordingly, once the VA is completed, the team must make suggested recommendations to reduce security risks.

Based on the vulnerabilities identified and the risk that the layers of security are breached, appropriate enhancements to the security countermeasures are recommended. Countermeasure options will be identified to further reduce vulnerability at the facility. These include improved countermeasures that follow the process security doctrines of deter, detect, delay, respond, mitigate and possibly prevent. Some of the factors to be considered are:

- Reduced probability of successful attack
- Degree of risk reduction by the options
- Reliability and maintainability of the options
- Capabilities and effectiveness of mitigation options
- Costs of mitigation options
- Feasibility of the options

The countermeasure options should be re-ranked to evaluate effectiveness, and prioritized to assist management decision making for implementing security program enhancements. The recommendations should be included in a VA report that can be used to communicate the results of the VA to management for appropriate action.

There is a need to follow-up on the recommended enhancements to the security countermeasures so they are properly reviewed, tracked, and managed until they are resolved. Resolution may include adoption of the VA team's recommendations, substitution of other improvements that achieve the same level of risk abatement, or rejection. Rejection of a VA recommendation and related acceptance of residual risk should be based on valid reasons that are well documented.

This VA process is summarized in Figure 1 and illustrated further in the flowcharts that follow in Figures 2a through 2c. Later in this chapter, preparation activities, such as data gathering and forming the VA team are described. Later sections provide details for each step in the RAMCAP VA methodology. These steps and associated tasks are also summarized in Figure 5.

BILLING CODE 4410–10–P

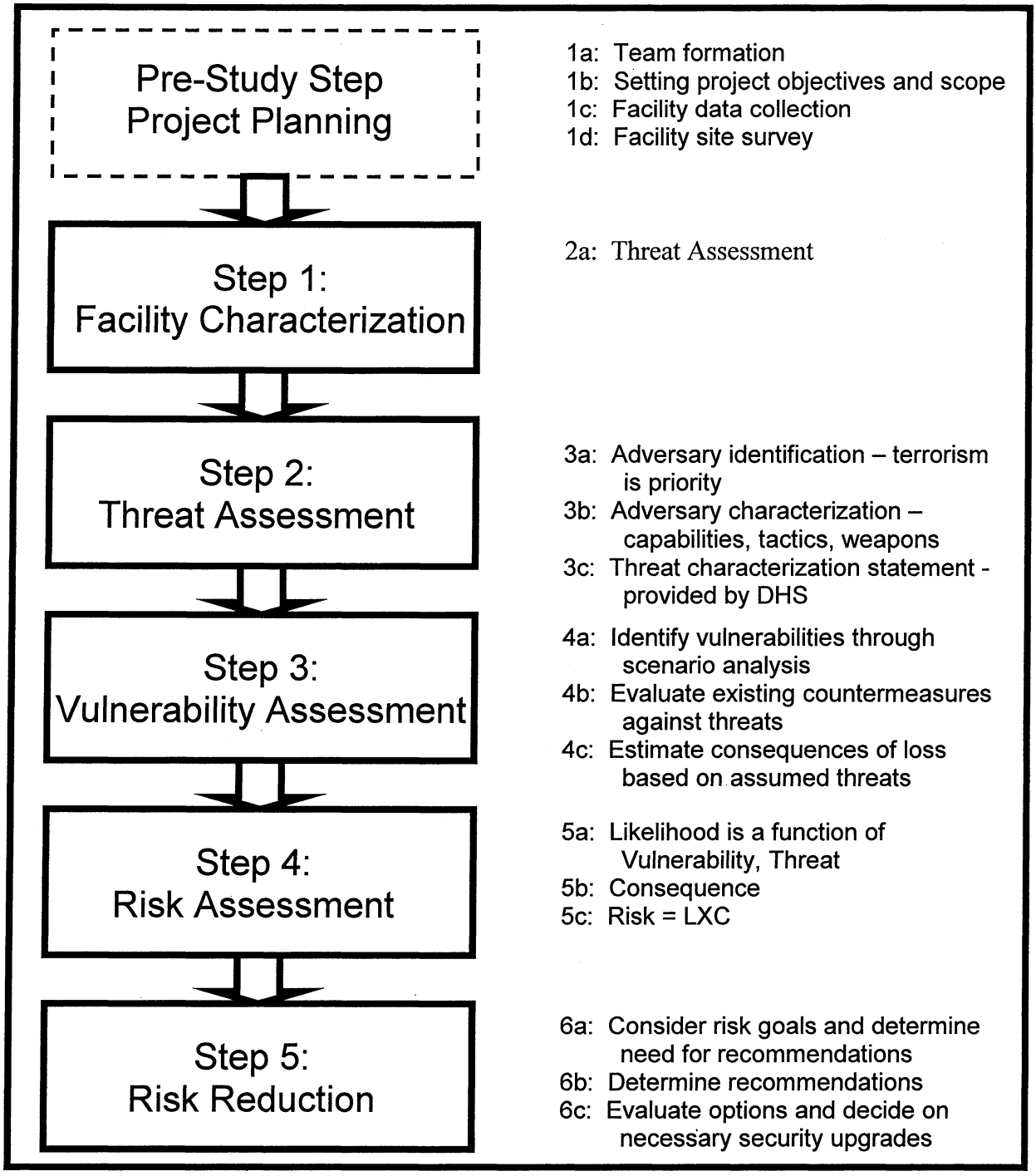

Pre-Study Step
Project Planning
1a: Team formation
1b: Setting project objectives and scope
1c: Facility data collection
1d: Facility site survey
Step 1:
Facility Characterization
2a: Threat Assessment
Step 2:
Threat Assessment
3a: Adversary identification – terrorism is priority
3b: Adversary characterization – capabilities, tactics, weapons
3c: Threat characterization statement - provided by DHS
Step 3:
Vulnerability Assessment
4a: Identify vulnerabilities through scenario analysis
4b: Evaluate existing countermeasures against threats
4c: Estimate consequences of loss based on assumed threats
Step 4:
Risk Assessment
5a: Likelihood is a function of Vulnerability, Threat
5b: Consequence
5c: Risk = LXC
Step 5:
Risk Reduction
6a: Consider risk goals and determine need for recommendations
6b: Determine recommendations
6c: Evaluate options and decide on necessary security upgrades

Figure 2a—RAMCAP Vulnerability Assessment Methodology—Step 1

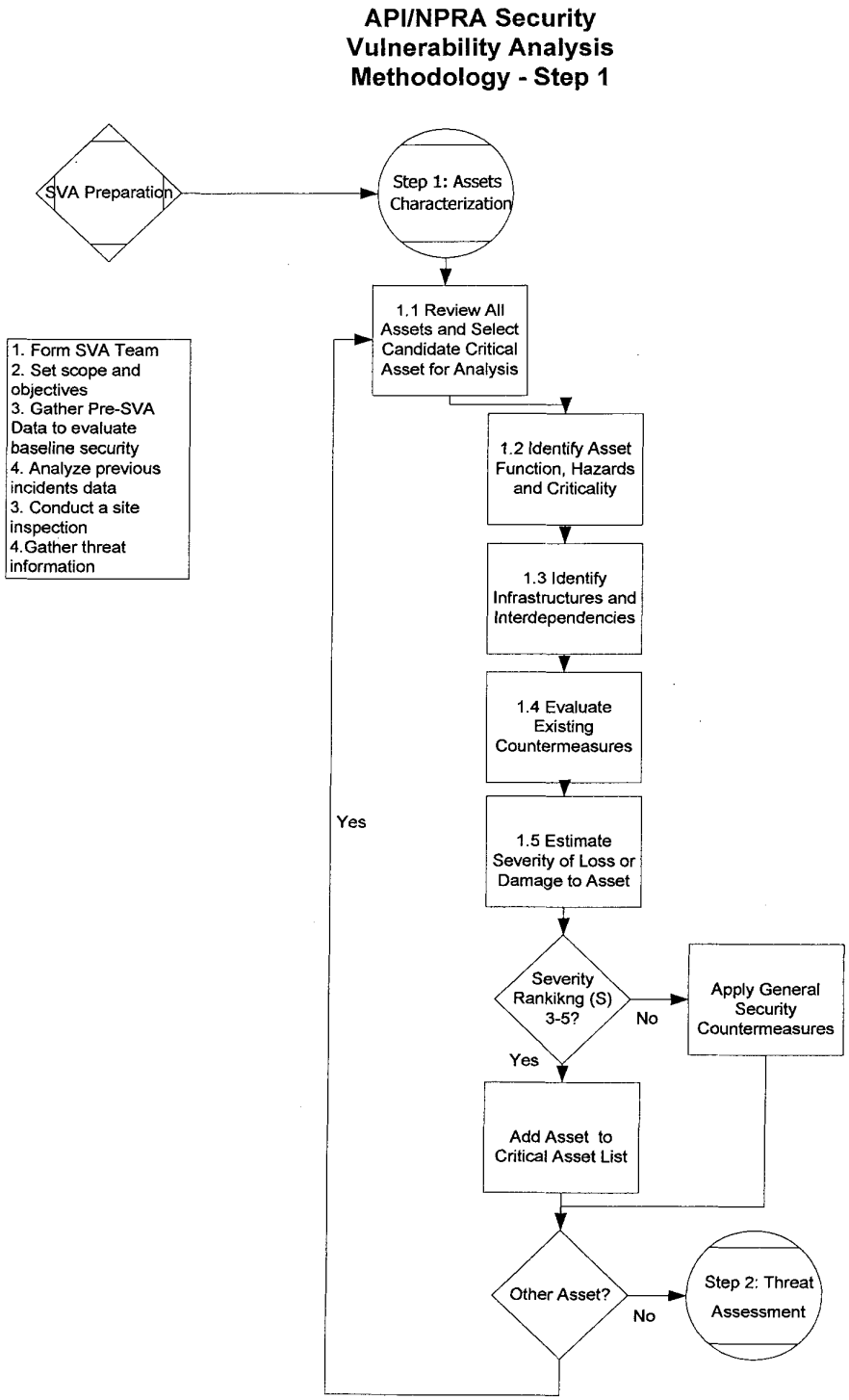
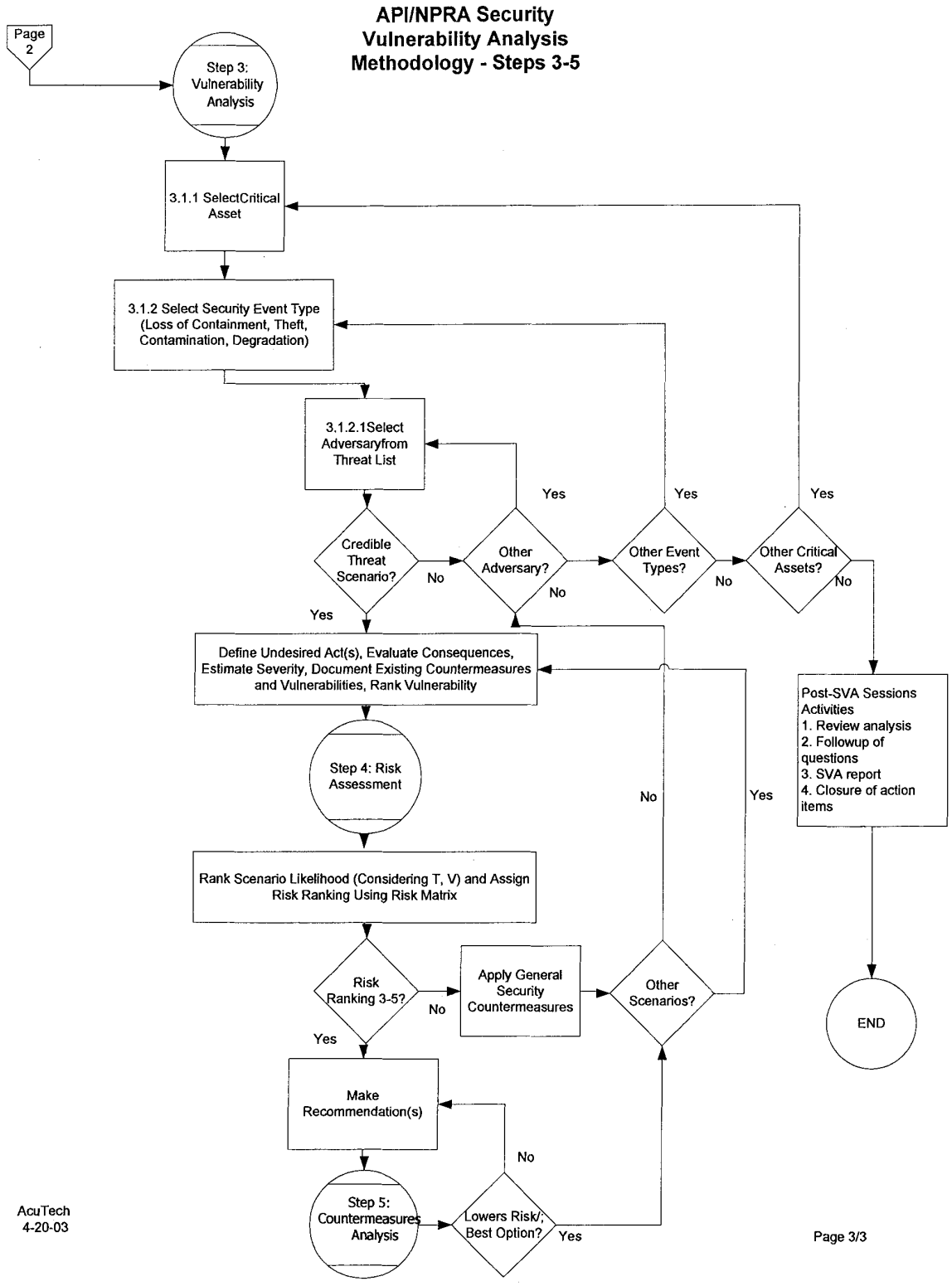


Figure 2b—RAMCAP Vulnerability Assessment Methodology—Step 2

Details of the Threat Assessment portion of the methodology are still being developed.

Figure 2c—RAMCAP Vulnerability Assessment Methodology—Steps 3–5



VA METHODOLOGY

Planning for Conducting an VA

Prior to conducting the VA team-based sessions, there are a number of activities that must be done to ensure an efficient and accurate analysis. There are many factors in successfully completing an VA including the following:

- The activity should be planned in advance;
- Have the full support and authorization by management to proceed;
- The data should be verified and complete;
- The objectives and scope should be concise;
- The team should be knowledgeable of and experienced at the process they are reviewing; and,
- The team leader should be knowledgeable and experienced in the VA process methodology.

All of the above items are controllable during the planning stage prior to conducting the VA sessions. Most important for these activities is the determination of VA-specific objectives and scope, and the selection and preparation of the VA Team.

Prerequisites to conducting the VA include gathering study data, gathering and analyzing threat information, forming a team, training the team on the method to be used, conducting a baseline security survey, and planning the means of documenting the process.

VA Team

The VA approach includes the use of a representative group of company experts plus outside experts if needed to identify potential security related events or conditions, the consequences of these events, and the risk reduction activities for the operator's system. These experts draw on the years of experience, practical knowledge, and observations from knowledgeable field operations and maintenance personnel in understanding where the security risks may reside and what can be done to mitigate or ameliorate them.

Such a company group typically consists of representation from: Company security, risk management, operations, engineering, safety, environmental, regulatory compliance, logistics/distribution, IT and other team members as required. This group of experts should focus on the vulnerabilities that would enhance the effectiveness of the site security plan. The primary goal of this group is to capture and build into the VA method the experience of this diverse group of individual experts so that the VA process will capture and incorporate information that may not be available in typical operator databases.

If the VA will include terrorism attacks on a process handling flammable, explosive, reactive or toxic substances, the VA should be conducted by a team with skills in both the security and process safety areas. This is because the team must evaluate traditional facility security as well as process safety-related vulnerabilities and countermeasures. The final security strategy for protection of the process assets from these events is likely to be a combination of security and process safety strategies.

It is expected that a full time ''core'' team is primarily responsible, and that they are led by a Team Leader. Other part-time team members, interviewees and guests are used as required for efficiency and completeness. At a minimum, VA teams should possess the knowledge and/or skills listed in Figure 3. Other skills that should be considered and included, as appropriate, are included as optional or part-time team membership or as guests and persons interviewed.

The VA Core Team is typically made up of three to five persons, but this is dependent on the number and type of issues to be evaluated and the expertise required to make those judgments. The Team Leader should be knowledgeable and experienced in the VA approach.

VA Objectives and Scope

The VA Team Leader should develop an objectives and scope statement for the VA. This helps to focus the VA and ensure completeness. An example VA objectives statement is shown in Figure 4.

A work plan should then be developed to conduct the VA with a goal of achieving the objectives. The work plan needs to include the scope of the effort, which includes which physical or cyber facilities and issues will be addressed.

Given the current focus on the need to evaluate terrorist threats, the key concerns are the intentional harm to critical infrastructure that may result in catastrophic consequences. For the RAMCAP methodology, the key events and consequences of interest include those described as key security events in the CCPS VA guidelines.[7] In addition to the security events recommended in those guidelines, the RAMCAP VA methodology recommends including injury to personnel and the public directly or indirectly.

Other events may be included in the scope, but it is prudent to address these four primary security events first since these are primarily events involving the processes that make the petroleum industry facilities unique from other facilities.

Figure 3—RAMCAP VA Team Members

The VA Core Team members should have the following skill sets and experience: • Team Leader – knowledge of and experience with the VA methodology; • Security representative – knowledge of facility security procedures, methods and systems; • Safety representative – knowledge of potential process hazards, process safety procedures, methods, and systems of the facility; • Facility representative - knowledge of the design of the facility under study including asset value, function, criticality, and facility procedures; • Operations representative – knowledge of the facility process and equipment operation; • Information Systems/Automation representative (for cyber security assessment) – knowledge of information systems technologies and cyber security provisions; knowledge of process control systems.
The VA Optional/Part-Time Team members may include the following skill sets and experience: • Security specialist – knowledge of threat assessment, terrorism, weapons, targeting and insurgency/guerilla warfare, or specialized knowledge of detection technologies or other countermeasures available; • Cyber security specialist – knowledge of cyber security practices and technologies; • Subject matter experts on various process or operations details such as process technologies, rotating equipment, distributed control systems, electrical systems, access control systems, etc.; • Process specialist – knowledge of the process design and operations • Management – knowledge of business management practices, goals, budgets, plans, and other management systems.

Figure 4—VA Sample Objectives Statement

To conduct an analysis to identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company.

Figure 5—RAMCAP VA Methodology, Security Events of Concern

Security Event Type	Candidate Critical Assets
Loss of Containment, Damage, or Injury	Loss of containment of process hydrocarbons or hazardous chemicals on the plant site from intentional damage of equipment or the malicious release of process materials, which may cause multiple casualties, severe damage, and public or environmental impact. Also included is injury to personnel and the public directly or indirectly
Theft	Hydrocarbon, chemical, or information theft or misuse with the intent to cause severe harm at the facility or offsite
Contamination	Contamination or spoilage of plant products or information to cause worker or public harm on or offsite;
Degradation of Assets	Degradation of assets or infrastructure or the business function or value of the facility or the entire company through destructive acts of terrorism.

Data Gathering, Review, and Integration

The objective of this step is to provide a systematic methodology for Owner/Operators to obtain the data needed to manage the security of their facility. Most Owner/Operators will find that many of the data elements suggested here are already being collected. This section provides a systematic review of potentially useful data to support a security plan. However, it should be recognized that all of the data elements in this section are not necessarily applicable to all systems.

The types of data required depend on the types of risks and undesired acts that are anticipated. The operator should consider not only the risks and acts currently suspected in the system, but also consider whether the potential exists for other risks and acts not previously experienced in the system, *e.g.*, bomb blast damage. This section includes lists of many types of data elements. The following discussion is separated into four subsections that address sources of data, identification of data, location of data, and data collection and review.

Annex 1 includes a list of potentially useful data that may be needed to conduct an VA.

Data Sources

The first step in gathering data is to identify the sources of data needed for facility security management.

These sources can be divided into four different classes.

1. Facility and Right of Way Records. Facility and right of way records or experienced personnel are used to identify the location of the facilities. This information is essential for determining areas and other facilities that either may impact or be impacted by the facility being analyzed and for developing the plans for protecting the facility from security risks. This information is also used to develop the potential impact zones and the relationship of such impact zones to various potentially exposed areas surrounding the facility *i.e.*, population centers, and industrial and government facilities.

2. System Information. This information identifies the specific function of the various parts of the process and their importance from a perspective of identifying the security risks and mitigations as well as understanding the alternatives to maintaining the ability of the system to continue operations when a security threat is identified. This information is also important from a perspective of determining those assets and resources available in-house in developing and completing a security plan. Information is also needed on those systems in place, which could support a security plan such as an integrity management program and IT security functions.

3. Operation Records. Operating data are used to identify the products transported and the operations as they may pertain to security issues to facilities and pipeline segments which may be impacted by security risks. This information is also needed to prioritize facilities and pipeline segments for security measures to protect the system, *e.g.*, type of product, facility type and location, and volumes transported. Included in operation records data gathering is the need to obtain incident data to capture historical security events.

4. Outside Support and Regulatory Issues. This information is needed for each facility or pipeline segment to determine the level of outside support that may be needed and can be expected for the security measures to be employed at each facility or pipeline segment. Data are also needed to understand the expectation for security preparedness and coordination from the regulatory bodies at the government, state, and local levels. Data should also be developed on communication and other infrastructure issues as well as sources of information regarding security threats, *e.g.*, ISACs (Information Sharing and Analysis Centers).

Identifying Data Needs

The type and quantity of data to be gathered will depend on the individual facility or pipeline system, the VA methodology selected, and the decisions that are to be made. The data collection approach will follow the VA path determined by the initial expert team assembled to identify the data needed for the first pass at VA. The size of the facility or pipeline system to be evaluated and the resources available may prompt the VA team to begin their work with

an overview or screening assessment of the most critical issues that impact the facility or pipeline system with the intent of highlighting the highest risks. Therefore, the initial data collection effort will only include the limited information necessary to support this VA. As the VA process evolves, the scope of the data collection will be expanded to support more detailed assessment of perceived areas of vulnerability.

Locating Required Data

Operator data and information are available in different forms and format. They may not all be physically stored and updated at one location based on the current use or need for the information. The first step is to make a list of all data required for vulnerability assessment and locate the data. The data and information sources may include:

- Facility plot plans, equipment layouts and area maps
- Process and Instrument Drawings (P&IDs)
- Pipeline alignment drawings
- Existing company standards and security best practices
- Product throughput and product parameters
- Emergency response procedures
- Company personnel interviews
- LEPC (Local Emergency Planning Commission) response plans
- Police agency response plans
- Historical security incident reviews
- Support infrastructure reviews

Data Collection and Review

Every effort should be made to collect good quality data. When data of suspect quality or consistency are encountered, such data should be flagged so that during the assessment process, appropriate confidence interval weightings can be developed to account for these concerns.

In the event that the VA approach needs input data that are not readily available, the operator should flag the absence of information. The VA team can then discuss the necessity and urgency of collecting the missing information.

Analyzing Previous Incidents Data

Any previous security incidents relevant to the vulnerability assessment may provide valuable insights to potential vulnerabilities and trends. These events from the site and, as available, from other historical records and references, should be considered in the analysis. This may include crime statistics, case histories, or intelligence relevant to facility.

Conducting a Site Inspection

Prior to conducting the VA sessions, it is necessary for the team to conduct a site inspection to visualize the facility and to gain valuable insights to the layout, lighting, neighboring area conditions, and other facts that may help understand the facility and identify vulnerabilities. The list of data requirements in Appendix A and the checklist in Appendix B may be referenced for this purpose.

Gathering Threat Information

The team should gather and analyze relevant company and industry and DHS (or other governmental) provided threat information, such as that available from the Energy ISAC, DHS, FBI, or other local law enforcement agency. At a minimum, the DHS-provided Threat Handbook should be thoroughly reviewed by all team members.

STEP 1: ASSETS CHARACTERIZATION

Characterization of the facility is a step whereby the facility assets and hazards are identified, and the potential consequences of damage or theft to those assets is analyzed. The focus is on processes which may contain petroleum or hazardous chemicals and key assets, with an emphasis on possible public impacts. This factor (severity of the consequences) is used to screen the facility assets into those that require only general vs. those that require more specific security countermeasures.

The team produces a list of candidate critical assets that need to be considered in the analysis. Attachment 1—Step 1: Critical Assets/Criticality Form is helpful in developing and documenting the list of critical assets. The assets may be processes, operations, personnel, or any other asset as described in Chapter 3.

Figure 6 below summarizes the key steps and tasks required for Step 1.

Step 1.1—Identify Critical Assets

The VA Team should identify critical assets for the site being studied. The focus is on petroleum or chemical process assets, but any asset may be considered. For example, the process control system may be designated as critical, since protection of it from physical and cyber attack may be important to prevent a catastrophic release or other security event of concern. Assets include the full range of both material and non-material aspects that enable a facility to operate.

FIGURE 6—RAMCAP VA METHODOLOGY, DESCRIPTION OF STEP 1 AND SUBSTEPS

Step	Task
Step 1: Assets Characterization	
1.1 Identify critical assets.	Identify critical assets of the facility including people, equipment, systems, chemicals, products, and information.
1.2 Identify critical functions.	Identify the critical functions of the facility and determine which assets perform or support the critical functions.
1.3 Identify critical infrastructures and interdependencies.	Identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset.
1.4 Evaluate existing countermeasures.	Identify what protects and supports the critical functions and assets. Identify the relevant layers of existing security systems including physical, cyber, operational, administrative, and business continuity planning, and the process safety systems that protect each asset.
1.5 Evaluate impacts.	Evaluate the hazards and consequences or impacts to the assets and the critical functions of the facility from the disruption, damage, or loss of each of the critical assets or functions.
1.6 Select targets for further analysis.	Develop a target list of critical functions and assets for further study.

FIGURE 7—RAMCAP VA METHODOLOGY, EXAMPLE CANDIDATE CRITICAL ASSETS

Security event type	Candidate critical assets
Loss of Containment, Damage, or Injury.	• Process equipment handling petroleum and hazardous materials including processes, pipelines, storage tanks. • Marine vessels and facilities, pipelines, other transportation systems. • Employees, contractors, visitors in high concentrations.
Theft	• Hydrocarbons or chemicals processed, stored, manufactured, or transported; • Metering stations, process control and inventory management systems. • Critical business information from telecommunications and information management systems including Internet accessible assets.

FIGURE 7—RAMCAP VA METHODOLOGY, EXAMPLE CANDIDATE CRITICAL ASSETS—Continued

Security event type	Candidate critical assets
Contamination	• Raw material, intermediates, catalysts, products, in processes, storage tanks, pipelines. • Critical business or process data.
Degradation of Assets.	• Processes containing petroleum or hazardous chemicals. • Business image and community reputation. • Utilities (Electric Power, Steam, Water, Natural Gas, Specialty Gases). • Telecommunications Systems. • Business systems.

The following information should be reviewed by the VA Team as appropriate for determination of applicability as critical assets:

• Any applicable regulatory lists of highly hazardous chemicals, such as the Clean Air Act 112(r) list of flammable and toxic substances for the EPA Risk Management Program (RMP) 40 CFR Part 68 or the OSHA Process Safety Management (PSM) 29 CFR 1910.119 list of highly hazardous chemicals;

• Inhalation poisons or other chemicals that may be of interest to adversaries.

• Large and small scale chemical weapons precursors as based on the following lists:

— Chemical Weapons Convention list;

— FBI Community Outreach Program (FBI List) for Weapons of Mass Destruction materials and precursors;

— The Australia Group list of chemical and biological weapons

• Material destined for the food, nutrition, cosmetic or pharmaceutical chains;

• Chemicals which are susceptible to reactive chemistry

Owner/Operators may wish to consider other categories of chemicals that may cause losses or injuries that meet the objectives and scope of the analysis. These may include other flammables, critically important substances to the process, explosives, radioactive materials, or other chemicals of concern.

In addition, the following personnel, equipment and information may be determined to be critical:

• Process equipment
• Critical data
• Process control systems
• Personnel
• Critical infrastructure and support utilities

Step 1.2—Identify Critical Functions

The VA Team should identify the critical functions of the facility and determine which assets perform or support the critical functions. For example, the steam power plant of a refinery may be critical since it is the sole source of steam supply to the refinery.

Step 1.3—Identify Critical Infrastructures and Interdependencies

The VA team should identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset. For example, the electrical substation may be the sole electrical supply to the plant, or a supplier delivers raw material to the facility via a single pipeline. The Interdependencies and Infrastructure Checklist can be used to identify and analyze these issues. Note that some of these issues may be beyond the control of the owner/operator, but it is necessary to understand the dependencies and interdependencies of the facility, and the result of loss of these systems on the process.

Step 1.4—Evaluate Existing Countermeasures

The VA team identifies and documents the existing security and process safety layers of protection. This may include physical security, cyber security, administrative controls, and other safeguards. During this step the objective is to gather information on the types of strategies used, their design basis, and their completeness and general effectiveness. A pre-VA survey is helpful to gather this information. The data will be made available to the VA team for them to form their opinions on the adequacy of the existing security safeguards during Step 3: Vulnerability Analysis and Step 5: Countermeasures Analysis.

A Countermeasures Survey Form can be used to gather information on the presence and status of existing safeguards or another form may be more suitable. Existing records and documentation on security and process safety systems, as well as on the critical assets themselves, can be referenced rather than repeated in another form of documentation. An example is included in Attachment 1.

The objective of the physical security portion of the survey is to identify measures that protect the entire facility and/or each critical asset of the facility, and to determine the effectiveness of the protection. Annex 2 contains checklists that may be used to conduct the physical security portion of the survey.

Note that the infrastructure interdependencies portion of the survey will identify infrastructures that support the facility and/or its critical assets (e.g., electric power, water, and telecommunications).

Step 1.5—Evaluate Impacts

The Impacts Analysis step includes both the determination of the hazards of the asset being compromised as well as the specific consequences of a loss. The VA team should consider relevant chemical use and hazard information, as well as information about the facility. The intent is to develop a list of target assets that require further analysis partly based on the degree of hazard and consequences. Particular consideration should be given to the hazards of fire, explosion, toxic release, radioactive exposure, and environmental contamination.

The consequences are analyzed to understand their possible significance. The Annex 1—Attachment 1—Step 1: Critical Assets/Criticality Form is useful to document the general consequences for each asset. The consequences may be generally described but consideration should be given to the selection listed in Figure 8. For DHS purposes, an VA will consider the consequences shown in Figure 9.

Figure 8—RAMCAP VA Methodology, Selected Possible Consequences of RAMCAP VA Security Events

Public fatalities or injuries
Site personnel fatalities or injuries
Large-scale disruption to the national economy, public or private operations
Loss of reputation or business viability

Figure 9 **Modified RAMCAP Consequence Parameters**
1. Human Health & Safety Impacts
a. Reported estimated residential population within the distance to the RMP toxic and flammable WCS endpoints (where EPA RMP is applicable)
b. Acute fatalities
c. Acute injuries
d. Theft of chemical weapons precursors/weapons of mass destruction onsite
e. Contamination to final food or pharmaceutical products made onsite
2. Economic Impacts
3. National Security & Government Functionality Impacts
a. Military mission importance
b. Delivery of public health services
c. Contamination/disruption to critical potable water or electrical energy services
4. Psychological Impacts
a. Impact to iconic/symbolic assets
b. High profile and/or symbolic casualties

The consequence analysis is done in a general manner. If the security event involves a toxic or flammable release to the atmosphere, the EPA RMP offsite consequence analysis guidance can be used as a starting point. If it is credible to involve more than the largest single vessel containing the hazardous material in a single incident, the security event may be larger than the typical EPA RMP worst-case analysis.

A risk ranking scale can be used to rank the degree of severity. Figure 10 illustrates a set of consequence definitions based on four categories of events: A. Fatalities and injuries; B. Environmental impacts; C. Property damage; and D. Business interruption. Asset owners may consider using a risk matrix such as this for making individual risk-based decisions for security, particularly if they use the RAMCAP VA methodology as a generalized vulnerability assessment tool.

BILLING CODE 4410–10–P

Figure 10—RAMCAP VA Methodology, Example Definitions of Consequences of the Event

DESCRIPTION	RANKING
A. Possible for any offsite fatalities from large-scale toxic or flammable release; possible for multiple onsite fatalities B. Major environmental impact onsite and/or offsite (e.g., large-scale toxic contamination of public waterway) C. Over $X property damage D. Very long term (> X years) business interruption/expense; Large-scale disruption to the national economy, public or private operations; Loss of critical data; Loss of reputation or business viability	S5 – Very High
A. Possible for onsite fatalities; possible offsite injuries B. Very large environmental impact onsite and/or large offsite impact C. Between $X – $Y property damage D. Long term (X months – Y years) business interruption/expense	S4 – High
A. No fatalities or injuries anticipated offsite; possible widespread onsite serious injuries B. Environmental impact onsite and/or minor offsite impact C. Between $X -$Y property damage D. Medium term (X months – Y months) business interruption/expense	S3 – Medium
A. Onsite injuries that are not widespread but only in the vicinity of the incident location; No fatalities or injuries anticipated offsite B. Minor environmental impacts to immediate incident site area only C. Between $X – $Y loss property damage D. Short term (up to X months) business interruption/expense	S2 – Low
A. Possible minor injury onsite; No fatalities or injuries anticipated offsite B. No environmental impacts C. Up to $X Property Damage D. Very short term (up to X weeks) business interruption/expense	S1 – Very Low

As part of the RAMCAP program, DHS has been interested in certain consequence and vulnerability information for a limited number of more critical national sites. For reporting this information to DHS, the following ranking process should be used for assessing consequences.

Figure 11
RAMCAP Consequence Ranges

RAMCAP Consequence Criteria	Consequence Categories										
	0	1	2	3	4	5	6	7	8	9	10
Number Of Fatalities	0 - 100	101 - 200	201 – 400	401 - 800	801 - 1,600	1,601 - 3,200	3,201 - 6,400	6,401 - 12,800	12,801 - 25,600	25,601 - 51,200	51,201 - 102,400
Number Of Injuries	0 - 300	501 - 1000	1001 - 2000	2001 - 4000	4001 - 8000	8001 - 16000	16001 - 32000	32001 - 64000	64001 - 128000	128001 - 256000	256001 - 512000
Economic Impacts	<$100M	$100M - $200M	$200M - $400M	$400M - $800M	$800M - $1.6B	$1.6B - $3.2B	$3.2B - $6.4B	$6.4B - $12.8B	$12.8B - $25.6B	$25.6B - $51.2B	$51.2B - $102.4B

The consequences of a security event at a facility are generally expressed in terms of the degree of acute health effects (*e.g.*, fatality, injury), property damage, environmental effects, etc. This definition of consequences is the same as that used for accidental releases, and is appropriate for security-related events. The key difference is that they may involve effects that are more severe than expected with accidental risk. This difference has been considered in the steps of the VA. The economic consequences for RAMCAP include direct replacement costs, business interruption, and the cost of cleanup and restoration.

The VA Team should evaluate the potential consequences of an attack using the judgment of the VA team. If scenarios are done, the specific consequences may be described in scenario worksheets.

Team members skilled and knowledgeable in the process technology should review any off-site consequence analysis data previously developed for safety analysis purposes or prepared for adversarial attack analysis. The consequence analysis data may include a wide range of release scenarios if appropriate.

Proximity to off-site population is a key factor since it is both a major influence on the person(s) selecting a target, and on the person(s) seeking to defend that target.

Step 1.6—Select Targets for Further Analysis

For each asset identified, the criticality of each asset must be understood. This is a function of the value of the asset, the hazards of the asset, and the consequences if the asset was damaged, stolen, or misused. For hazardous chemicals, consideration may include toxic exposure to workers or the community, or potential for the misuse of the chemical to produce a weapon or the physical properties of the chemical to contaminate a public resource.

The VA Team develops a Target Asset List that is a list of the assets associated with the site being studied that are more likely to be targets, based on the complete list of assets and the identified consequences and targeting issues identified in the previous steps. During Step 3: Vulnerability Analysis, the Target Asset List will be generally paired with specific threats and evaluated against the potential types of attack that could occur.

The RAMCAP VA methodology uses ranking systems that are based on a scale of 1–5 where 1 is the lowest value and 5 is the highest value. Based on the consequence ranking and criticality of the asset, the asset is tentatively designated a candidate critical target asset.

STEP 2: THREAT ASSESSMENT

This step involves identifying appropriate threat scenarios for the SVA based on a DHS provided sector-level Threat Assessment that provides an overall assessment of the potential threats to the CI/KR sectors, as well as analysis of how these threats relate to sector vulnerabilities and consequences.

Threat assessment is an important part of a security management system, especially in light of the emergence of international terrorism in the United States. There is a need for understanding the threats facing the industry and any given facility or operation to properly respond to those threats.

A threat assessment is used to evaluate the likelihood of adversary activity against a given asset or group of assets. It supports the establishment and prioritization of security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability and intent.

The assessment should identify threat categories and potential adversaries, such as insiders, external agents (outsiders), and collusion between insiders and outsiders. The SVA team should consider each type of adversary identified in the threat assessment and their assessed level of capability and motivation.

To be effective, threat assessment must be considered a dynamic process, whereby the threats are continuously evaluated for change. During any given SVA exercise, the threat assessment is referred to for guidance on general or specific threats.

Examples of threats are set forth on the following table (Fig. 12):

BILLING CODE 4410–10–P

Readers are advised: the RAMCAP postulated threats, developed by and currently in use by industry, are for illustrative purposes only. Certain threats set forth below would not be applicable to the chemical security program at issue.

Figure 12
RAMCAP Postulated Threat Scenarios

Maritime (Boat as weapon)				
1. Delivery	Small boat (pleasure or Zodiac) <10ft draft	Fast Boat <10 ft draft	Barge	Deep draft shipping 20-40 ft draft
Explosive	Explosive charge 400 lbs TNT equivalent	Explosive charge 2000 lbs (TNT equivalent)	Explosive charge -10000 lbs (TNT equivalent)	Explosive charge 40,000 lbs (TNT equivalent) LNG, LPG, weaponized

Land VBIED (w/out assault team)				
2. Single VBIED	Car bomb 400lbs TNT equivalent	Van Bomb 1000lbs TNT equivalent	Mid-size Truck Bomb 10,000lbs TNT equivalent	Large Truck Bomb (18 wheeler) 40,000lbs TNT equivalent

What do they do? Attempt to maximize death/destruction through most productive direct means. For example, aiming at critical assets in hard targets, or clusters of people for open populated areas, or structural supports that would bring down people.

Assault				
Assault force size	1	2-4	5-8	9-16
3. Delivery system **"Land"**	Pedestrian, all-terrain vehicle, motorcycle, over the road personnel transport, cargo truck	All-terrain vehicles, motorcycles, over the road personnel transport, cargo truck	All-terrain vehicles, motorcycles, over the road personnel transport, cargo truck,	All-terrain vehicles, motorcycles, over the road personnel transport, Cargo truck,
4. Delivery system **"Air"**	N/A	1 Helicopter Pilot + 1-3 attack force	2 Helicopters 2 pilots + 4-6 attack force	3 Helicopters 3 pilots + 7-13 attack force
5. Delivery	Lone swimmer	1 x small boat	1 x small boat (Zodiac)	2 x small boat Zodiac

Figure 12
RAMCAP Postulated Threat Scenarios

system **"Water"**		(Zodiac)	(personnel) 1 x small/medium cargo watercraft (equipment)	Medium cargo watercraft (equipment)
Weapons	Pistol, assault rifle, light machine gun	Pistols, assault rifles, sniper rifles (.50 caliber), light machine guns	Pistols, submachine guns, assault rifles, sniper rifles (.50 caliber), light machine guns, rocket propelled grenades (RPG)	Pistols, submachine guns, assault rifles, sniper rifles (.50 caliber), light machine guns, rocket propelled grenades (RPG)
Explosives	Grenades (H.E. & Incendiary) Explosive vest/or satchel.	Grenades (H.E. & Incendiary) Bulk explosives, VBIED (400lb TNT equivalent) for access or attack	Grenades (H.E. & Incendiary) Bulk explosives, VBIED (400lb TNT equivalent) for access or attack Specialized Explosive charges (Breaching charges, shape charges, ballistic discs)	Grenades (H.E. & Incendiary) Bulk explosives, 2 VBIEDs (400lb TNT equivalent) for access or attack Specialized Explosive charges (Breaching charges, shape charges, ballistic discs) Anti-personnel mines
Tools	Minimal breaching tools	Mechanical breaching tools, required hand tools	Mechanical breaching tools, quick saws, chainsaws, sledge hammers, required hand tools	Mechanical breaching tools, quick saws, chainsaws, sledge hammers, required hand tools
Weight per person	65 pounds	65 pounds	65 pounds	65 pounds
What do they do inside? Attempt to maximize death/damage through most productive direct means. For example, in a nuclear plant, they try to achieve sabotage the reactor and breach containment. For the mall, they try to kill as many as possible directly. Assume suicide intent.				
Process Sabotage				
7. Cyber				
8. Insider threat				
9. Unauthorized access				
What do they do? Cause harm through process control systems, though contamination, etc.				
Diversion of sensitive property (theft)				
10. Cyber				
11.Insider threat				
12. Unauthorized access				
What do they do? Steal information, dangerous substances, valuable resources, etc.				

The threat assessment is not based on perfect information and will be developed in the absence of site-specific information on threats. A suggested approach is to make an assumption that international terrorism is possible at every facility.

VA STEP 3: VULNERABILITY ANALYSIS

The Vulnerability Analysis step involves three steps. Once the VA Team has determined how an event can be induced, it should determine how an adversary could make it occur. There are two schools of thought on methodology: the scenario-based approach and the asset-based approach. Both approaches are identical in the beginning, but differ in the degree of detailed analysis of threat scenarios and specific countermeasures applied to a given scenario. The assets are identified, and the consequences are analyzed as per Step 2, for both approaches. Both approaches result in a set of annotated potential targets, and both approaches may be equally successful at evaluating security vulnerabilities and determining required protection.

Figure 13—RAMCAP VA Methodology, Description of Step 3 and Sub-steps

Step	Task
Step 3: Vulnerability Analysis	
3.1 Define scenarios and evaluate specific consequences	Use scenario-analysis and/or use asset-based analysis to document the adversary's potential actions against an asset
3.2 Evaluate effectiveness of existing security measures	Identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary.
3.3 Identify vulnerabilities and estimate degree of vulnerability	Identify the potential vulnerabilities of each critical asset to applicable threats or adversaries. Estimate the degree of vulnerability of each critical asset for each threat-related undesirable event or incident and thus each applicable threat or adversary.

Step 3.1—Define Scenarios and Evaluate Specific Consequences

Each asset in the list of critical target assets from Step 2 is reviewed in light of the threat assessment, and the relevant threats and assets are paired in a matrix or other form of analysis, as shown in Attachment 1—Steps 3–5 RAMCAP VA Methodology—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form. The importance of this step is to develop a design basis threat statement for each facility.

Once the VA Team has determined how a malevolent event can be induced, it should determine how an adversary could execute the act.

The action in the Scenario-based approach follow the VA method as outlined in Chapter 3. To establish an understanding of risk, scenarios can be assessed in terms of the severity of consequences and the likelihood of occurrence of security events. These are qualitative analyses based on the judgment and deliberation of knowledgeable team members.

Step 3.2—Evaluate Effectiveness of Existing Security Measures

The VA Team will identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary.

Step 3.3—Identify Vulnerabilities and Estimate Degree of Vulnerability

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and the subsequent destruction or theft of an asset. Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices.

For each asset, the vulnerability or difficulty of attack is considered using the definitions shown in Figure 14. For RAMCAP purposes, the asset owner also is asked to evaluate the likelihood of successful attack against the prescribed postulated threat scenarios at a minimum using the definitions shown in Figure 15.

The Scenario-based approach is identical to the Asset-based approach in the beginning, but differs in the degree of detailed analysis of threat scenarios. The scenario-based approach uses a more detailed analysis strategy and brainstorms a list of scenarios to understand how the undesired event might be accomplished. The scenario-based approach begins with an onsite inspection and interviews to gather specific information for the VA Team to consider.

The following is a description of the approach and an explanation of the contents of each column of the worksheet in Attachment 1—Steps 3–5 RAMCAP VA Methodology—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form.

Figure 14—RAMCAP VA Methodology, Vulnerability Rating Criteria

Vulnerability Level	Description
5 - Very High	Indicates that there are no effective protective measures currently in place to Deter, Detect, Delay, and Respond to the threat and so an adversary would easily be capable of exploiting the critical asset.
4 – High	Indicates there are some protective measures to Deter, Detect, Delay, or Respond to the asset but not a complete or effective application of these security strategies and so it would be relatively easy for the adversary to successfully attack the asset.
3 – Medium	Indicates that although there are some effective protective measures in place to Deter, Detect, Delay, and Respond, there isn't a complete and effective application of these security strategies and so the asset or the existing countermeasures could likely be compromised.
2 – Low	Indicates that there are effective protective measures in place to Deter, Detect, Delay, and Respond, however, at least one weakness exists that an adversary would be capable of exploiting with some effort to evade or defeat the countermeasure given substantial resources.
1 - Very Low	Indicates that multiple layers of effective protective measures to Deter, Detect, Delay, and Respond to the threat exist and the chance that the adversary would be able to exploit the asset is very low.

VULNERABILITY (Likelihood of Adversary Success)				Cat	CONSEQUENCE CATEGORIES										
Descriptor	Range	Representative Likelihood			0	1	2	3	4	5	6	7	8	9	10
Adversary is almost certain to succeed	0.5 - 1	> 50/50		5											
Adversary's chances of success about even	0.25 - 0.5	~1 in 3		4											
Adversary might succeed - but less than 50/50 chance	0.125 - 0.25	~1 in 5		3											
Adversary is probably not going to succeed	0.0625 - 0.125	~1 in 10		2											
Extremely Unlikley	0.0312 - 0.0625	~1 in 20		1											
Ext Impossible	<0.0312	< 1 in 50		0											
Number Of Fatalities					0 - 100	101 - 200	201 - 400	401 - 800	801 - 1,600	1,601 - 3,200	3,201 - 6,400	6,401 - 12,800	12,801 - 25,600	25,601 - 51,200	51,201 - 102,400
Number Of Injuries					0 - 300	501 - 1000	1001 - 2000	2001 - 4000	4001 - 8000	8001 - 16000	16001 - 32000	32001 - 64000	64001 - 128000	128001 - 256000	256001 - 512000
Economic Impacts					<$100M	$100M - $200M	$200M - $400M	$400M - $800M	$800M - $1.6B	$1.6B - $3.2B	$3.2B - $6.4B	$6.4B - $12.8B	$12.8B - $25.6B	$25.6B - $51.2B	$51.2B - $102.4B

The VA Team devises a scenario based on their perspective of the consequences that may result from undesired security events given a postulated threat for a given asset. This is described as an event sequence including the specific malicious act or cause and the potential consequences, while considering the challenge to the existing countermeasures. It is conservatively assumed that the existing countermeasures are exceeded or fail in order to achieve the most serious consequences, in order to understand the hazard. When considering the risk, the existing countermeasures need to be assessed as to their integrity, reliability, and ability to deter, detect, and delay.

In this column the type of malicious act is recorded. As described earlier, the four types of security events included in the objectives of an VA at a minimum include:

1. Theft/Diversion of material for subsequent use as a weapon or a component of a weapon
2. Causing the deliberate loss of containment of a chemical present at the facility
3. Contamination of a chemical, tampering with a product, or sabotage of a system
4. An act causing degradation of assets, infrastructure, business and/or value of a company or an industry.

Given the information collected in Steps 1–3 regarding the site's key target assets, and the existing layers and rings of protection, a description of the initiating event of a malicious act scenario may be entered into the Undesired Event column. The VA team brainstorms the vulnerabilities based on the information collected in Steps 1–3. The VA team should brainstorm vulnerabilities for all of the malicious act types that are applicable at a minimum. Other scenarios may be developed as appropriate.

Completing the Worksheet

The next step is for the team to evaluate scenarios concerning each asset/threat pairing as appropriate. The fields in the worksheet are completed as follows:

1. Asset: The asset under consideration is documented. The team selects from the targeted list of assets and considers the scenarios for each asset in turn based on priority.
2. Security Event Type: This column is used to describe the general type of malicious act under consideration. At a minimum, the four types of acts previously mentioned should be considered as applicable.
3. Threat Category: The category of adversary including terrorist, activist, disgruntled employee, etc.
4. Type: The type of adversary category whether (I)—Insider, (E)—External, or (C)—Colluded threat.
5. Undesired Act: A description of the sequence of events that would have to occur to breach the existing security measures is described in this column.
6. Consequences: Consequences of the event are analyzed and entered into the Consequence column of the worksheet. The consequences should be conservatively estimated given the intent of the adversary is to maximize their gain. It is recognized that the severity of an individual event may vary considerably, so VA teams are encouraged to understand the expected consequence of a successful attack or security breach.
7. Consequences Ranking: Severity of the Consequences on a scale of 1–5. The severity rankings are assigned based on a conservative assumption of a successful attack.
8. Existing Countermeasures: The existing security countermeasures that relate to detecting, delaying, or deterring the adversaries from exploiting the vulnerabilities may be listed in this column. The countermeasures have to be functional (i.e., not bypassed or removed) and sufficiently maintained as prescribed (i.e., their ongoing integrity can be assumed to be as designed) for credit as a countermeasure.
9. Vulnerability: The specific countermeasures that would need to be circumvented or failed should be identified.
10. Vulnerability Ranking: The degree of vulnerability to the scenario rated on a scale of 1–5.
11. L(ikelihood): The likelihood of the security event is assigned a qualitative ranking in the likelihood column. The likelihood rankings are generally assigned based on the likelihood associated with the entire scenario, assuming that all countermeasures are functioning as designed/intended. Likelihood is a team decision and is assigned from the Likelihood scale based on the factors of Vulnerability and Threat for the particular scenario considered.
12. R(isk): The severity and likelihood rankings are combined in a relational manner to yield a risk ranking. The development of a risk ranking scheme, including the risk ranking values is described in Step 4.
13. New Countermeasures: The recommendations for improved countermeasures that are developed are recorded in the New Countermeasures column.

STEP 4: RISK ANALYSIS/RANKING

In either the Asset-based or the Scenario-based approach to Vulnerability Analysis, the next step is to determine the level of risk of the adversary exploiting the asset given the existing security countermeasures. Figure 16 lists the sub-steps.

The scenarios are risk-ranked by the VA Team based on a simple scale of 1–5. The risk matrix shown in Figure 17 could be used to plot each scenario based on its likelihood and consequences. The intent is to categorize the assets into discrete levels of risk so that appropriate countermeasures can be applied to each situation.

Note: For this matrix, a Risk Ranking of ''5 x 5'' represents the highest severity and highest likelihood possible.

3.7 STEP 5: IDENTIFY COUNTERMEASURES

A Countermeasures Analysis identifies shortfalls between the existing security and the desirable security where additional recommendations may be justified to reduce risk. In assessing the need for additional countermeasures, the team should ensure each scenario has the following countermeasures strategies employed:

- DETER an attack if possible
- DETECT an attack if it occurs
- DELAY the attacker until appropriate authorities can intervene
- RESPOND to neutralize the adversary, to evacuate, shelter in place, call local authorities, control a release, or other actions.

The VA Team evaluates the merits of possible additional countermeasures by listing them and estimating their net effect on the lowering of the likelihood or severity of the attack. The team attempts to lower the risk to the corporate standard.

Figure 16—RAMCAP VA Methodology, Description of Step 4 and Substeps

Step	Task
Step 4: Risk Assessment	
4.1 Estimate risk of successful attack	As a function of consequence and probability of occurrence, determine the relative degree of risk to the facility in terms of the expected effect on each critical asset (a function of the consequences or impacts to the critical functions of the facility from the disruption or loss of the critical asset, as evaluated in Step 1) and the likelihood of a successful attack (a function of the threat or adversary, as evaluated in Step 2, and the degree of vulnerability of the asset, as evaluated in Step 3).
4.2 Prioritize risks	Prioritize the risks based on the relative degrees of risk and the likelihoods of successful attacks.

Figure 17—RAMCAP VA Methodology, Risk Ranking Matrix

SEVERITY						
LIKELIHOOD		5	4	3	2	1
	5	High	High	High	Med	Med
	4	High	High	Med	Med	Low
	3	High	Med	Med	Low	Low
	2	Med	Med	Low	Low	Low
	1	Med	Low	Low	Low	Low

Figure 18—RAMCAP VA Methodology, Description of Step 5 and Substeps

Step	Task
Step 5: Countermeasures Analysis	
5.1 Identify and evaluate enhanced countermeasures options	Identify countermeasures options to further reduce the vulnerabilities and thus the risks while considering such factors as: • Reduced probability of successful attack • The degree of risk reduction provided by the options; • The reliability and maintainability of the options; • The capabilities and effectiveness of these mitigation options; • The costs of the mitigation options; • The feasibility of the options. Rerank to evaluate effectiveness.
5.2 Prioritize potential enhancements	Prioritize the alternatives for implementing the various options and prepare recommendations for decision makers

FOLLOW-UP TO THE VA

The outcome of the VA is:

- the identification of security vulnerabilities;
- a set of recommendations (if necessary) to reduce risk to an acceptable level.

The VA results should include a written report that documents:

- The date of the study;
- The study team members, their roles and expertise and experience;
- A description of the scope and objectives of the study;
- A description of or reference to the VA methodology used for the study;
- The critical assets identified and their hazards and consequences;
- The security vulnerabilities of the facility;
- The existing countermeasures;
- A set of prioritized recommendations to reduce risk;

Once the report is released, it is necessary for a resolution management system to resolve issues in a timely manner and to document the actual resolution of each recommended action.

Attachment 1—Example RAMCAP VA Methodology Forms

The following four forms can be used to document the VA results. Blank forms are provided, along with a sample of how each form is to be completed. Other forms of documentation that meet the intent of the VA guidance can be used.

BILLING CODE 4410–10–P

Step 1: RAMCAP VA Methodology - Critical Assets/Criticality Form

Facility Name:

Critical Assets	Criticality/Hazards	Asset Severity Ranking
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

Step 3–5: RAMCAP VA Methodology – Vulnerability Analysis/Risk Ranking/Countermeasures Form

Facility Name:

Critical Assets:

Security Event Type	Threat Category	Type	Undesired Act	Consequences	S	Existing Countermeasures	Vulnerability	V	L	R	New Countermeasures

Glossary of Terms

Adversary: Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. An adversary could include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can include site insiders, site outsiders, or the two acting in collusion.

Alert levels: Describes a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent, based on government or company intelligence information. Different security measures may be implemented at each alert level based on the level of threat to the facility.

Asset: An asset is any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets in the VA include the community and the environment surrounding the site.

Asset category: Assets may be categorized in many ways. Among these are:

- People
- Hazardous materials (used or produced)
- Information
- Environment
- Equipment
- Facilities
- Activities/Operations
- Company reputation

Benefit: Amount of expected risk reduction based on the overall effectiveness of countermeasures with respect to the assessed vulnerabilities.

Capability: When assessing the capability of an adversary, two distinct categories need to be considered. The first is the capability to obtain, damage, or destroy the asset. The second is the adversary's capability to use the asset to achieve their objectives once the asset is obtained, damaged, or destroyed.

Checklist: A list of items developed on the basis of past experience that is intended to be used as a guide to assist in applying a standard level of care for the subject activity and to assist in completing the activity in as thorough a manner.

Consequences: The amount of loss or damage that can be expected, or may be expected from a successful attack against an asset. Loss may be monetary but may also include political, morale, operational effectiveness, or other impacts. The impacts of security events which should be considered involve those that are extremely severe. Some examples of relevant consequences in an VA include fatality to member(s) of the public, fatality to company personnel, injuries to member(s) of the public, injuries to company personnel, large-scale disruption to public or private operations, large-scale disruption to company operations, large-scale environmental damage, large-scale financial loss, loss of critical data, and loss of reputation.

Cost: Includes tangible items such as money and equipment as well as the operational costs associated with the implementation of countermeasures. There are also intangible costs such as lost productivity, morale considerations, political embarrassment, and a variety of others. Costs may be borne by the individuals who are affected, the corporations they work for, or they may involve macroeconomic costs to society.

Cost-Benefit analysis: Part of the management decision-making process in which the costs and benefits of each countermeasure alternative are compared and the most appropriate alternative is selected. Costs include the cost of the tangible materials, and also the on-going operational costs associated with the countermeasure implementation.

Countermeasures: An action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) (intent and/or capability) as well as the asset's value. The cost of a countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

Countermeasures analysis: A comparison of the expected effectiveness of the existing countermeasures for a given threat against the level of effectiveness judged to be required in order to determine the need for enhanced security measures.

Cyber security: Protection of critical information systems including hardware, software, infrastructure, and data from loss, corruption, theft, or damage.

Delay: A countermeasures strategy that is intended to provide various barriers to slow the progress of an adversary in penetrating a site to prevent an attack or theft, or in leaving a restricted area to assist in apprehension and prevention of theft.

Detection: A countermeasures strategy that is intended to identify an adversary attempting to commit a security event or other criminal activity in order to provide real-time observation as well as post-incident analysis of the activities and identity of the adversary.

Deterrence: A countermeasures strategy that is intended to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Physical security systems such as warning signs, lights, uniformed guards, cameras, bars are examples of countermeasures that provide deterrence.

Hazard: A situation with the potential for harm.

Intelligence: Information to characterize specific or general threats, including the intent and capabilities of adversaries.

Intent: A course of action that an adversary intends to follow.

Layers of protection: A concept whereby several independent devices, systems, or actions are provided to reduce the likelihood and severity of an undesirable event.

Likelihood of adversary success: The potential for causing a catastrophic event by defeating the countermeasures. LAS is an estimate that the security countermeasures will thwart or withstand the attempted attack, or if the attack will circumvent or exceed the existing security measures. This measure represents a surrogate for the conditional probability of success of the event.

Mitigation: The act of causing a consequence to be less severe.

Physical security: Security systems and architectural features that are intended to improve protection. Examples include fencing, doors, gates, walls, turnstiles, locks, motion detectors, vehicle barriers, and hardened glass.

Process Hazard Analysis (PHA): A hazard evaluation of broad scope that identifies and analyzes the significance of hazardous situations associated with a process or activity.

Response: The act of reacting to detected or actual criminal activity either immediately following detection or post-incident.

Risk: The potential for damage to or loss of an asset. Risk, in the context of process security, is the potential for a catastrophic outcome to be realized. Examples of the catastrophic outcomes that are typically of interest include an intentional release of hazardous materials to the atmosphere, or the theft of hazardous materials that could later be used as weapons, or the contamination of hazardous materials that may later harm the public, or the economic costs of the damage or disruption of a process.

Risk assessment: Risk (R) assessment is the process of determining the likelihood of an adversary (T) successfully exploiting vulnerability (V) and the resulting degree of consequences (C) on an asset. A risk assessment provides the basis for rank ordering of risks and thus establishing priorities for the application of countermeasures.

Safeguard: Any device, system or action that either would likely interrupt the chain of events following an initiating event or that would mitigate the consequences.[4]

Security layers of protection: Also known as concentric ''rings of protection'', a concept of providing multiple independent and overlapping layers of protection in depth. For security purposes, this may include various layers of protection such as counter-surveillance, counterintelligence, physical security, and cyber security.

Security management system checklist: A checklist of desired features used by a facility to protect its assets.

Security plan: A document that describes an owner/operator's plan to address security issues and related events, including security assessment and mitigation options. This includes security alert levels and response measures to security threats.

Vulnerability Assessment (VA): An VA is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact. VAs are not a quantitative risk analysis, but are performed qualitatively using the best judgment of security and safety professionals. The determination of risk (qualitatively) is the desired outcome of the VA, so that it provides the basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures.

Technical Security: Electronic systems for increased protection or for other security

purposes including access control systems, card readers, keypads, electric locks, remote control openers, alarm systems, intrusion detection equipment, annunciating and reporting systems, central stations monitoring, video surveillance equipment, voice communications systems, listening devices, computer security, encryption, data auditing, and scanners.

Terrorism: The FBI defines terrorism as, ''the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives.''

Threat: Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Threat categories: Adversaries may be categorized as occurring from three general areas:

- Insiders
- Outsiders
- Insiders working in collusion with outsiders

Undesirable events: An event that results in a loss of an asset, whether it is a loss of capability, life, property, or equipment.

Vulnerabilities: Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational and personnel practices.

Abbreviations and Acronyms

ACC—American Chemistry Council
AIChE—American Institute of Chemical Engineers
API—American Petroleum Institute
AWCS—Accidental Worst-Case Scenario
C—Consequence
CCPS—Center for Chemical Process Safety of the American Institute of Chemical Engineers (AIChE)
CCTV—Closed Circuit Television
CEPPO—Chemical Emergency Preparedness and Prevention Office (USEPA)
CMP—Crisis Management Plan
CSMS—Chemical Security Management System
CW—Chemical Weapons
CWC—Chemical Weapons Convention
D—Difficulty of Attack
DCS—Distributed Control Systems
DHS—Department of Homeland Security
DOE—Department of Energy
DOT—U.S. Department of Transportation
EHS—Environmental, Health, and Safety
EPA—U.S. Environmental Protection Agency
ERP—Emergency Response Process
EHS—Environmental, Health, and Safety
FBI—U.S. Federal Bureau of Investigation
FC—Facility Characterization
HI—Hazard Identification
HSAS—Homeland Security Advisory System
IPL—Independent Protection Layer
IT—Information Technology
LA—Likelihood of Adversary Attack
LAS—Likelihood of Adversary Success
LOPA—Layer of Protection Analysis
MARSEC—Maritime Security Levels
MOC—Management of Change
NPRA—National Petrochemical and Refiners Association
OSHA—Occupational Safety and Health Administration
PHA—Process Hazard Analysis
PLC—Programmable Logic Controller
PSI—Process Safety Information
PSM—Process Safety Management (Also refers to requirements of 29 CFR 1910.119)
R—Risk
RAMCAP—Risk Analysis and Management for Critical Asset Protection
RMP—Risk Management Process (Also refers to requirements of EPA 40 CFR Part 68)
S—Severity of the Consequences
SOCMA—Synthetic Organic Chemical Manufacturers Association
SOP—Standard Operating Procedure
T—Threat
TSA—Transportation Security Administration
V—Vulnerability
VA—Vulnerability Assessment
WMD—Weapons of Mass Destruction

BILLING CODE 4410–10–P

ANNEX A — VA Supporting Data Requirements

RAMCAP VA Methodology Supporting Data	
Category*	**Description**
A	Scaled drawings of the overall facility and the surrounding community (e.g., plot plan of facility, area map of community up to worst case scenario radius minimum)
A	Aerial photography of the facility and surrounding community (if available)
A	Information such as general process description, process flow diagrams, or block flow diagrams that describes basic operations of the process including raw materials, feedstocks, intermediates, products, utilities, and waste streams.
A	Information (e.g., drawings that identify physical locations and routing) that describes the infrastructures upon which the facility relies (e.g., electric power, natural gas, petroleum fuels, telecommunications, transportation [road, rail, water, air], water/wastewater)
A	Previous security incident information
A	Description of guard force, physical security measures, electronic security measures, security policies
A	Threat information specific to the company (if available)
B	Specifications and descriptions for security related equipment and systems. Plot plan showing existing security countermeasures
B	RMP information including registration and offsite consequence analysis (if applicable, or similar information)
B	Most up-to-date PHA reports for processes considered targets
B	Emergency response plans and procedures (site, community response, and corporate contingency plans)
B	Information on material physical and hazard properties (MSDS).
B	Crisis management plans and procedures (site and corporate)

B	Complete an VA chemicals checklist to determine whether the site handles any chemicals on the following lists:
C	• EPA Risk Management Program (RMP) 40 CFR Part 68;
C	• OSHA Process Safety Management (PSM) 29 CFR 1910.119;
C	• Chemical Weapons Convention, Schedule 2 and specifically listed Schedule 3 chemicals;
C	• FBI Community Outreach Program (FBI List) for WMD precursors;
C	• The Australia Group list of chemical and biological weapons.
C	Design basis for the processes (as required)
C	Unit plot plans of the processes
C	Process flow diagrams (PFDs) and piping and instrument diagrams (P&IDs) for process streams with hazardous materials
C	Safety systems including fire protection, detection, spill suppression systems
C	Process safety systems including safety instrumented systems (SIS), PLC's, process control systems
C	Operating procedures for start-up, shutdown, and emergency (operators may provide general overview of this information, with written information available as required.
C	Mechanical equipment drawings for critical equipment containing highly hazardous chemicals
C	Electrical one-line diagrams
C	Control system logic diagrams
C	Equipment data information
C	Information on materials of construction and their properties
C	Information on utilities used in the process
C	Test and maintenance procedures for security related equipment and systems

*Categories: A = Documentation to be provided to VA team as much in advance as possible before arrival for familiarization;
B = Documentation to be gathered for use in VA team meetings on site;
C = Documentation that should be readily available on an as-needed basis.

Acknowledgements

"Chemical Accident Prevention Provisions" (part 68 of Title 40 of the Code of Federal Regulations (CFR)).

Chemical Facility Vulnerability Assessment Methodology, NIJ Special Report, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July, 2002.

Counterterrorism and Contingency Planning Guide. Special publication from Security Management magazine and American Society for Industrial Security, 2001.

Guidance Document for Implementing 40 CFR Part 68, USEPA, 1998.

Guidelines for Chemical Process Quantitative Risk Analysis, Second Ed., Center for Chemical Process Safety, American Institute of Chemical Engineers, 2000.

Guidelines for Consequence Analysis of Chemical Releases, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1999.

Guidelines for Technical Management of Chemical Process Safety, Center for Chemical

Process Safety, American Institute of Chemical Engineers, 1998.

Guidelines for Technical Planning for On-Site Emergencies, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1996.

Inherently Safer Chemical Processes A Life Cycle Approach, Center for Chemical Process Safety, American Institute of Chemical Engineers, 1996.

Layers of Protection Analysis, Center for Chemical Process Safety, American Institute of Chemical Engineers, 2001

''Site Security Guidelines for the U.S. Chemical Industry'', American Chemistry Council, October, 2001.

Bowers, Dan M., ''Security Fundamentals for the Safety Engineer'', *Professional Safety*, American Society of Safety Engineers, December, 2001, pgs. 31–33.

Dalton, Dennis. *Security Management: Business Strategies for Success.* (Newton, MA: Butterworth-Heinemann Publishing, 1995).

Fischer, Robert J. and Green, Gion. *Introduction to Security*, 6th ed. (Boston: Butterworth-Heinemann, 1998).

Ragan, Patrick T., *et al.*, ''Chemical Plant Safety'', *Chemical Engineering Progress*, February, 2002, pgs. 62–68.

Roper, C.A. *Physical Security and the Inspection Process* (Boston: Butterworth-Heinemann, 1997).

Roper, C.A. *Risk Management for Security Professionals* (Boston: Butterworth-Heinemann, 1999).

Walsh, Timothy J., and Richard J. Healy, eds. *Protection of Assets Manual* (Santa Monica, CA: Merritt Co.). Four-volume loose-leaf reference manual, updated monthly.

[FR Doc. 06–9903 Filed 12–27–06; 8:45 am]

BILLING CODE 4410–10–C